Ari Marcelo Liotto

GERENCIAMENTO DE RISCO

A Aderência da Metodologia do TCU à Metodologia COSO

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Controle Externo - Área de Auditoria Governamental.

Orientador: Luiz Akutsu

Co-Orientador: Marcelo Luiz Souza da Eira

Brasília, DF

2004

RESUMO

O tema focal desta monografia é a utilização do conceito de risco em auditorias. É feita uma abordagem de alguns conceitos fundamentais, tais como: auditoria, controle interno, risco, materialidade, evidência e, principalmente, risco de auditoria. Buscam-se conceitos não somente acadêmicos, mas também de entidades responsáveis por contabilidade e auditoria, dando-se ênfase, sempre que possível, àqueles provenientes de Entidades de Fiscalização Superior.

Auditoria é vista, numa visão bastante abrangente, como "o ato de se confrontar a condição – situação encontrada – com o critério – situação que deve ser" (ARAÚJO, 1998, p15). São apresentados diversos conceitos de controles internos que os relacionam com as políticas e procedimentos desenvolvidos pela gerência de uma entidade para auxiliar no alcance de seus objetivos.

Risco numa visão simples pode ser entendido como qualquer evento capaz de impedir ou atrapalhar o alcance de objetivos definidos. Assim, risco de auditoria é qualquer evento capaz de atrapalhar ou impedir que o objetivo de auditoria, dar um informe fiel acerca da confrontação critério x situação, seja alcançado.

O risco de auditoria é composto por três componentes. Risco inerente, que é o risco do negócio, que nasce com as atividades desenvolvidas pela entidade e se mantém o mesmo caso não existiam controles internos para mitigá-lo. Risco de controle, que se relaciona com a possibilidade de que falhas dos sistemas de controle interno não detectem erros relevantes. E risco de detecção que é aquele relacionado ao próprio trabalho do auditor, à possibilidade de que suas ações não detectem erros, omissões ou irregularidades existentes.

Verifica-se uma lacuna nos procedimentos de fiscalização do TCU, que é a não utilização do conceito de risco de auditoria, principalmente, o de risco de detecção. Com isso, não se explicita que o processo de auditoria, como qualquer outro, está sujeito a riscos, e que, portanto, a opinião dada não apresenta infalibilidade.

Aborda-se a questão do gerenciamento de risco em instituições, e, para tanto, é feita uma apresentação pormenorizada do documento *Enterprise Risk Management Framework* ("Modelo para Gerenciamento de Riscos Empresariais") do COSO. Esse documento, ainda em fase de minuta, é resultado de um projeto com objetivo de criar um modelo, conceitualmente robusto, que possa ser utilizado pelos dirigentes no desenvolvimento do gerenciamento de risco de suas entidades.

Ao fornecer um método para que se efetive o gerenciamento de risco em organizações, o documento apresenta uma série de conceitos bastante úteis quando o ponto de vista é o de auditar instituições com a visão voltada para os seus riscos inerentes.

Dessa forma, realiza-se a comparação entre a metodologia COSO e a Metodologia de Análise de Risco para Escolha de Temas de Fiscalização, utilizada pelo TCU no processo de definição de áreas e temas passíveis de serem fiscalizados em determinadas instituições. A conclusão é pela existência de diferenças entre as metodologias, sendo a mais significativa a questão envolvendo a realização de avaliação dos principais controles gerenciais sem realizar uma avaliação prévia dos riscos e das respostas aos riscos correspondentes, conforme previsto na metodologia COSO.

SUMÁRIO

1. Introdução----------07

2. Revisão de Literatura----------09

2.1. Conceituação de Auditoria----------09

2.2. Conceituação de Controle Interno----------13

2.3. Controles Internos conforme o COSO----------16

2.4. Definição de Riscos----------19

2.5. Materialidade, Risco de Auditoria e Evidência----------22

2.6. Gerenciamento de Risco----------29

3. Exposição da Metodologia de Gerenciamento de Risco Empresarial (*Enterprise Risk Management Framework)* do COSO---------- 33

3.1. Ambiente Interno---------- 39

3.2. Definição de Objetivos----------45

3.3. Identificação de Eventos----------49

3.4. Avaliação de Risco---------- 53

3.5. Resposta ao Risco----------56

3.6. Atividades de Controle----------58

3.7. Informação e Comunicação---------- 62

3.8. Monitoramento----------67

3.9. Limitações do Gerenciamento de Risco Empresarial----------72

3.10. Papéis e Responsabilidades----------73

4. Metodologia de Análise de Risco para Escolha de Temas de Fiscalização do TCU----------77

4.1. Identificação dos Objetivos da Entidade e Responsabilidades Gerenciais – Etapa I----------77

4.2. Análise Externa – Etapa II----------81

4.3. Avaliação dos Controles Gerenciais - Etapa III

Determinação das áreas Estratégicas de Risco da Entidade - Etapa IV---------- 83

4.4. Priorização das Áreas de Risco e Apontamento do Tipo de Fiscalização Requerida – Etapa V

Avaliação do Risco das Fiscalizações Sugeridas - Etapa VI

Submissão das Propostas ao Plenário - Etapa VII----------86

5. Conclusão--89

Referências--91

1. Introdução

> Risco é a expressão da probabilidade de ocorrência e do impacto de eventos futuros incertos que têm potencial para influenciar o alcance dos objetivos de uma organização. Em termos simples e não acadêmicos, risco é todo evento que pode atrapalhar ou impedir que se atinja o alvo pretendido (TCU, 2003, p.3).

Em um processo de auditoria, risco se relaciona com a possibilidade do auditor emitir uma opinião que não reflita a realidade analisada.

Para uma entidade qualquer, seja ela pública ou privada, com ou sem fins lucrativos, o risco se relaciona à não consecução dos objetivos dessa entidade.

Em 1992, foi publicado pelo COSO[1] um estudo denominado *Internal Control – Integrated Framework*[2]. Esse trabalho veio a se tornar referência mundial no que concerne à forma das entidades encararem a análise de riscos e desenvolver uma adequada estrutura de controles internos capaz de mitigar esses riscos.

Recentemente, no segundo semestre de 2003, o COSO disponibilizou, em sua página na Internet (http://www.coso.org), para consulta e comentários, a versão preliminar ("draft") de um novo estudo denominado *Enterprise Risk Management Framework*[3]. Esse documento faz parte de um projeto que objetiva desenvolver um modelo conceitualmente robusto capaz de prover princípios integrados, terminologia comum e um guia de implementação prática que dê suporte aos programas de desenvolvimento de processos de gerenciamento de risco ou à comparação dos processos existentes nas entidades (COSO, 2003a, tradução nossa).

Nesta monografia são expostos os conceitos e métodos presentes no documento *Enterprise Risk Management Framework*, do COSO, entendendo que, a exemplo do documento *Internal Control – Integrated Framework*, virá a ser um padrão mundial no que concerne à análise e ao gerenciamento de riscos empresariais.

Também é exposta a metodologia em uso no TCU relacionada ao conceito de risco (Metodologia de Análise de Risco para Escolha de Temas de Fiscalização). A

---

[1] COSO é a sigla de Committee of Sponsoring Organizations da National Comission on Fraudlent Financial Reporting, também conhecida como Treadeway Comission. Criada em 1985, é uma entidade do setor privado, sem fins lucrativos, voltada para o aperfeiçoamento da qualidade de relatórios financeiros por meio de éticas profissionais, implementação de controles internos e governança corporativa. São cinco as organizações norte-americanas que patrocinam o citado comitê: American Institute of Certified Public Accountants – AICPA; American Accounting Association – AAA, The Institute of Internal Auditors - IIA, Institute of Management Accountants - IMA e Financial Executives Institute – FEI.

[2] "Controles Internos – Um Modelo Integrado"

[3] "Modelo para Gerenciamento do Risco Empresarial"

questão de pesquisa central está relacionada à investigação do grau de aderência da metodologia do TCU à metodologia COSO.

A comparação entre essas metodologias se dá no campo conceitual, não havendo a intenção de se definir uma nova metodologia para o TCU. A aceitação das idéias expostas poderá levar à expansão do trabalho, com a adaptação da metodologia atual do Tribunal.

Este trabalho pretende assim, em resposta à questão de pesquisa formulada, dar uma visão sobre a importância para o auditor do entendimento do conceito de risco, seja dada sua indissociabilidade do trabalho de auditoria, seja devido à necessidade que as entidades têm de conhecer, de analisar e de gerenciar seus riscos.

2. Revisão da Literatura

2.1 Conceituação de Auditoria

O termo auditoria é objeto de diversas conceituações, que variam de acordo com a abordagem que se pretenda estabelecer.

Assim é que certos autores classificam a auditoria como uma especialização da contabilidade. Para Attie (1998, p.25) "a auditoria é uma especialização contábil voltada a testar a eficiência e eficácia do controle patrimonial implantado com o objetivo de expressar uma opinião sobre determinado dado". Já Sá entende que:

> Auditoria é uma tecnologia contábil aplicada ao sistemático exame dos registros, demonstrações e de quaisquer informes ou elementos de consideração contábil, visando a apresentar opiniões, conclusões, críticas e orientações sobre situações ou fenômenos patrimoniais da riqueza aziendal, pública ou privada, quer ocorridos, quer por ocorrer ou prospectados ou diagnosticados (SÁ, 2002, p.25).

Sá (2002, p.26), ao explicar sua conceituação, discorre sobre a necessidade da auditoria "buscar as suas normas práticas dentro dos postulados da Contabilidade por uma questão de hierarquia lógica".

Ao se analisar essas definições, observa-se, realmente, uma indissociação da auditoria à contabilidade, uma vez que a auditoria buscaria testar, na primeira definição, ou examinar sistematicamente, na segunda, os registros contábeis efetuados acerca de um certo patrimônio com fins de emissão de opinião acerca da contabilização desse patrimônio, ou, diretamente, acerca do próprio patrimônio.

O Conselho Federal de Contabilidade (CFC), ao discorrer sobre o conceito de auditoria nas Normas de Auditoria Independente das Demonstrações Contábeis - NBC T 11, assim se expressa:

> A auditoria das demonstrações contábeis constitui o conjunto de procedimentos técnicos que tem por objetivo a emissão de parecer sobre a sua adequação, consoante os Princípios Fundamentais da Contabilidade e as Normas Brasileiras de Contabilidade, e no que for pertinente, a legislação específica (CFC, 1997, p.2).

Para a *International Federation of Accountants*[4] (IFAC) (2001, p.148) "o objetivo de uma auditoria de demonstrações financeiras é o de permitir ao auditor expressar uma opinião sobre se as demonstrações financeiras foram elaboradas, em todos os aspectos significativos, de acordo com normas preestabelecidas" (tradução nossa).

[4] Federação Internacional dos Contadores

Ambas as definições são voltadas para o universo das auditorias independentes, que têm sob sua responsabilidade a emissão de um parecer sobre os demonstrativos contábeis. Há uma vinculação total entre auditoria e contabilidade, explicitada pelo CFC, e induzida pelo IFAC ao falar em "normas preestabelecidas".

Outra entidade de classe, a *American Accounting Association*[5] (AAA), define auditoria como:

> Um processo sistemático de obtenção e avaliação objetivas de evidências sobre afirmações a respeito de ações e eventos econômicos, para aquilatação do grau de correspondência entre as afirmações e critérios estabelecidos, e de comunicação dos resultados a usuários interessados (ACCOUNTING REVIEW apud BOYNTON E OUTROS, 2002, p. 30).

Essa definição apresenta-se mais ampla do que as anteriores, não limitando as demonstrações contábeis como o foco da auditoria, nem o universo da contabilidade como o critério estabelecido para a comparação das evidências obtidas. Mas, ainda limita o campo de ação quando relaciona somente "afirmações a respeito de ações e eventos econômicos", excluindo outras áreas de interesse para análise.

Uma conceituação extensiva é a apresentada por Araújo:

> A auditoria pode ser conceituada como um conjunto de procedimentos aplicados sobre determinadas ações, objetivando verificar se elas foram ou são realizadas em conformidade com normas, regras, orçamentos e objetivos. É o ato de se confrontar a condição – situação encontrada – com o critério – situação que deve ser (ARAÚJO, 1998, p. 15).

O maior mérito dessa definição está no seu poder de síntese ao definir auditoria como o ato de confrontação entre a condição e o critério, ao mesmo tempo em que é ampla por não restringir tipos de condição e critério.

Na verdade, o que torna cada uma das conceituações apresentadas ou diferentes ou agrupáveis é o objeto a que a auditoria se destina. Assim é que as definições de Attie e Sá tratam da auditoria contábil, também chamada de auditoria das demonstrações contábeis, pelo CFC, ou das demonstrações financeiras, pelo IFAC. A definição do AAA, embora de uma entidade de classe de contadores, é mais abrangente, podendo ser utilizada para fins mais variados. Araújo definiu auditoria em um sentido *lato*, para adiante, em sua obra, restringir o conceito a partir da definição de tipos de auditoria.

Para Araújo (1998) as auditorias se dividem em governamentais, quando se debruçam sobre a *res publica,* e privadas, com âmbito na iniciativa particular, no tocante ao campo de atuação. Internas, aquelas executadas por profissionais empregados da própria entidade auditada, e externas, executadas por profissionais externos à

empresa auditada, quanto à forma de realização. E contábeis ou financeiras, operacionais ou de otimização de recursos e integradas, no que concerne aos objetivos do trabalho. As contábeis ou financeiras são as que se destinam a apresentar um parecer sobre as demonstrações contábeis. As operacionais ou de otimização de recursos se referem à avaliação do desempenho e eficácia das operações, dos sistemas de informação e de organização e dos métodos de administração. As integradas são aquelas em que, além da realização dos aspectos envolvidos nas duas primeiras, é efetuado o exame de conformidade.

Já Boynton e outros (2002) definem três tipos de auditorias. A de demonstrações contábeis, que visa à emissão de um parecer sobre a adequação da apresentação dessas demonstrações. A de *compliance* (conformidade), na qual é feita a verificação se as atividades financeiras ou operacionais da entidade obedecem a condições, regras ou regulamentos a elas aplicáveis. E a operacional, em que se verifica a eficiência e eficácia das atividades operacionais da entidade, em comparação com objetivos estabelecidos. Os autores fazem, também, a distinção de três tipos de auditores. Os independentes, que operam por conta própria, ou são membros de empresas de auditoria, e realizam qualquer uma das três modalidades de auditoria. Os internos, que são empregados das organizações que auditam, e realizam, principalmente, auditorias de conformidade e operacional. E os públicos, que sendo empregados por entidades governamentais, engajam-se nos três tipos de auditoria.

Tais classificações são de interesse por mostrarem que o universo da auditoria é mais amplo do que as definições até agora apresentadas, as quais se referem, basicamente, à auditoria contábil ou financeira ou de demonstrações contábeis. Portanto, é relevante se buscar outras conceituações que envolvam as auditorias das modalidades interna e governamental.

Attie assim define auditoria interna:

> Auditoria interna é uma função independente de avaliação, criada dentro de uma empresa para examinar e avaliar suas atividades, como um serviço a essa mesma organização. A proposta da auditoria interna é auxiliar os membros da organização a desincumbirem-se eficazmente de suas responsabilidades. Para tanto, a auditoria interna lhes fornece análise, avaliações, recomendações, assessoria e informações relativas às atividades examinadas (ATTIE, 1992, p. 28).

---

[5] Associação Americana de Contadores

Uma noção importante da definição apresentada é que a auditoria interna é uma função independente em uma empresa. Ela organiza-se como uma atividade específica, um elemento no organograma da entidade, com função de avaliar o quão eficaz é a atuação dos membros dessa entidade, na consecução de suas responsabilidades.

Para o CFC (1995 apud ARAÚJO, 1998, p. 20) "a auditoria interna constitui o conjunto de procedimentos técnicos que têm por objetivo examinar a integridade, a adequação e a eficácia dos controles internos e das informações fiscais, contábeis, financeiras e operacionais da entidade".

Essa conceituação do CFC realça o caráter contábil da auditoria interna, devendo-se destacar a explicitação da função de exame da integridade, adequação e eficácia dos controles internos. Trata-se de papel relevante da auditoria interna, que será objeto de discussão posterior neste texto.

Uma definição mais atual de auditoria interna, pelos conceitos que traduz, é a do *The Institute of Internal Auditors*[6] (IIA):

> Auditoria Interna é uma atividade independente, de fornecimento de segurança objetiva e de consultoria que visa a acrescentar valor a uma organização e melhorar suas operações. Trazendo para a organização uma abordagem sistemática e disciplinada para avaliação e melhora da eficácia de seus processos de gerenciamento de risco, controle e governança, ajuda a atingir seus objetivos (IIA, 1999 apud BOYNTON E OUTROS, 2002, p.932).

Destacam-se na conceituação do IIA a preocupação com a geração de valor, e o auxílio no alcance dos objetivos de uma organização. São temas mais atuais, que se traduzem na explicitação da avaliação e melhora da eficácia dos processos de gerenciamento de risco, controles internos e governança de uma entidade. Todos esses temas serão objeto de discussão mais aprofundada neste texto.

Com relação à auditoria governamental, Sá (2002) diz se tratar de uma especialização dentro do campo da auditoria, seguindo todos os seus princípios técnicos básicos, mas com peculiaridades quanto à aplicação e com sistemática específica. Para o autor, todas as entidades do Poder Público, sejam da administração direta ou indireta subordinam-se a exames especiais relativos à gerência de patrimônios públicos.

Voltando-se para definições de auditoria de organismos responsáveis ou envolvidos com a execução de auditorias governamentais, apresenta-se a definição em sentido *lato* dada pela International Organization of Supreme Audit Institutions[7]

[6] Instituto dos Auditores Internos
[7] Organização Internacional das Entidades de Fiscalização Superior

(INTOSAI), conceituação que foi reproduzida pelo Tribunal de Contas da União (TCU) e pelo Tribunal de Contas de Portugal em seus manuais de auditoria:

> Auditoria é o exame das operações, atividades e sistemas de determinada entidade, com vista a verificar se são executados ou funcionam em conformidade com determinados objetivos, orçamentos, regras e normas (INTOSAI, 1986 apud TRIBUNAL DE CONTAS DE PORTUGAL, 1999, p.23).

Mais especificamente no que concerne à auditoria externa, assim se pronuncia a INTOSAI, acompanhada pelos Tribunais de Contas de Portugal e do Brasil:

> Auditoria externa é a auditoria realizada por um organismo externo e independente da entidade fiscalizada, tendo por objetivo, por um lado, emitir um parecer sobre as contas e a situação financeira, a legalidade e regularidade das operações e/ou sobre a gestão e, por outro, elaborar os relatórios correspondentes (INTOSAI, 1986 apud TCU, 1995, p. 3).

O conceito de auditoria externa é mais específico do que o conceito *lato* quanto à forma de realização – para usar a classificação de Araújo (1998) anteriormente exposta – já que o ente fiscalizador é externo e independente ao fiscalizado. No entanto, quanto à ação de auditoria em si, é mais amplo, pois, além da questão da conformidade ("legalidade e regularidade das operações") abre a possibilidade de pronunciamento sobre a gestão do ente fiscalizado (auditoria de gestão). Cita, ainda, a confecção de relatórios, nos quais são feitas recomendações e/ou determinações aos entes fiscalizados, de acordo com as características e atribuições de cada Entidade de Fiscalização Superior (EFS). Com isso, faz uma diferença marcante com o trabalho das auditorias independentes que, apesar de, também, serem externas, concluem seu trabalho com a emissão de um parecer, padronizado e mais simples, sobre as demonstrações contábeis do auditado. Sendo assim, essa conceituação reflete melhor a realidade dos trabalhos de auditoria que são realizados nas EFS, a exemplo do TCU.

2.2 Conceituação de Controle Interno

Não por acaso, as primeiras definições de auditoria apresentadas neste texto estavam amplamente relacionadas com a contabilidade. Na verdade, pelo fato da auditoria poder ser considerada uma especialização contábil, as suas normas e os seus procedimentos usualmente surgiram e continuam sendo desenvolvidos, em grande parte, por entidades ligadas à contabilidade. Assim, mesmo que certas modalidades de auditoria, principalmente aquelas ligadas à área governamental, se distanciem de certa

forma de conceitos mais rígidos da contabilidade, é significativo buscar nessa ciência definições a serem usadas no universo da auditoria.

Florentino (1975, p.103), ao discorrer sobre os objetivos da contabilidade cita, além dos de registro e medição do patrimônio, os de controle e análise. Para o autor "o simples princípio em que a contabilidade se baseia – o de registros duplos, já em si representa um excepcional sistema automático de controle". Vai mais além:

> O controle contábil, entretanto, alarga-se para um campo muito maior que o simplesmente contido em seu princípio teórico. Assim é que ao planejar os diferentes tipos de registros operacionais da empresa, o especialista contábil estabelece automaticamente uma rede de controles internos para a empresa, visando quer a segurança da exatidão dos registros contra erros ou omissões, quer a segurança contra desvios ou fraudes, quer a possibilidade de a qualquer momento reconstruir ou analisar os valores registrados. Daí surgem rotinas, formulários, separação de funções, contas especiais de controle, livros descentralizados, etc. (FLORENTINO, 1975, p.103).

Essa conceituação é importante para mostrar que qualquer entidade que possua sistema contábil tem desenvolvido algum tipo de sistema de controle interno, mesmo que de forma não consciente.

Para o CFC:

> O sistema contábil e de controles internos compreende o plano de organização e o conjunto integrado de método e procedimentos adotados pela entidade na proteção do seu patrimônio, promoção da confiabilidade e tempestividade dos seus registros e demonstrações contábeis, e de sua eficácia operacional (CFC, 1997, p.6).

Para outra entidade de classe de contadores, o *American Institute of Certified Public Accountants*[8] (AICPA) (AICPA apud ARAÚJO, 1998, p. 157) "o controle interno compreende o plano de organização e todos os métodos e medidas coordenados, adotados pela empresa para proteger seus ativos, verificar a exatidão operacional e promover a obediência às diretrizes administrativas estabelecidas".

Essas definições indicam que o controle interno é um sistema, criado pela empresa e de sua responsabilidade, composto por uma estrutura organizada e, preferencialmente formal, de divisão de trabalho, de autoridade e de responsabilidades dentro da entidade, o que constitui seu plano de organização, aliado a um conjunto de atitudes e processos relacionados a esse plano de organização visando o alcance de certos objetivos. Tais objetivos são: a proteção do patrimônio (bens, direitos e interesses) da empresa contra a utilização indevida ou malversação; o registro e contabilização adequada das suas transações e atividades, com a conseqüente

preparação e apresentação fidedigna de suas demonstrações contábeis; o estabelecimento de limites até os quais os diversos níveis de pessoal possam responder pela entidade, dinamizando a tomada de decisão; e a segurança de que as decisões e políticas da administração da entidade estão sendo adequadamente implantadas e respeitadas.

Quando da conceituação de auditoria interna realizada previamente, foi destacada a importante função de avaliação dos controles internos existentes. Na realidade, é comum a confusão entre esses dois conceitos, sendo que Araújo (1998), assim se pronuncia a esse respeito:

> De logo, vale citar que não se deve confundir auditoria interna com controle interno. Enquanto este representa um conjunto de políticas e procedimentos implantados pela administração, objetivando a salvaguarda dos ativos, a correta valoração dos passivos, a adequação das informações e a eficácia operacional, aquela é, apenas, um dos componentes do sistema de controle e que muito contribui para o alcance dos resultados almejados pelo sistema de controle interno (ARAÚJO, 1998, p. 156).

Destaca-se do entendimento do autor, o fato da auditoria interna ser parte do sistema de controles internos de uma entidade, sistema esse cuja responsabilidade pela criação é da administração dessa entidade. Assim não há que se falar em controles internos criados pela auditoria interna. Cabe a este órgão da estrutura organizacional avaliar a eficácia e eficiência dos procedimentos criados por outrem, mesmo por que, se a auditoria interna fosse responsável pela criação de controles, não possuiria a independência necessária para criticá-los.

No que concerne à auditoria governamental, a INTOSAI, no Glossário de termos e expressões utilizados em matéria de auditoria externa das finanças públicas, de 1986, assim define controles internos:

> Todo o sistema de controles financeiros e de qualquer outra natureza da entidade auditada, incluindo a estrutura organizacional, os métodos, os procedimentos e a auditoria interna, estabelecidos pelos administradores segundo os objetivos da entidade, que contribuem para que ela seja regularmente administrada de forma econômica, eficiente e eficaz, garantindo, assim a observância das políticas determinadas pela administração, salvaguardando bens e recursos, assegurando a fidedignidade e integridade dos registros contábeis e produzindo informações financeiras e gerenciais confiáveis e tempestivas (INTOSAI, 1986 apud ARAÚJO, 1998, p. 157).

Trata-se de uma definição abrangente, que versa sobre todos os aspectos tratados nas outras definições apresentadas. Não se limita a controles financeiros, mas “de

---

[8] Instituto Americano de Contadores Públicos Certificados

qualquer outra natureza", inclui o plano de organização ("estrutura organizacional, métodos e procedimentos"), explicitando a auditoria interna como componente do controle interno. Define-o como responsabilidade dos administradores, que devem criá-lo para auxiliar na consecução do objetivo de bem gerir a entidade. Por fim, relaciona todos os objetivos específicos citados nas outras definições: observância de políticas internas; salvaguarda de ativos; fidedignidade de registros; e informes contábeis.

2.3 Controles Internos conforme o COSO

Antes de se comentar a definição de controles internos existente no documento *Internal Control - Integrated Framework*, conhecido como Relatório COSO, é importante contextualizar rapidamente os motivos da criação desse documento nos Estados Unidos da América.

Para Boynton e outros (2002), autores norte-americanos, a importância dos controles internos para os gestores e para os auditores sempre foi reconhecida pela literatura profissional. Já em 1947, o AICPA registrava fatores que contribuíam para a importância do tema: a crescente complexidade das organizações; a possibilidade de redução de ocorrência de erros e irregularidades; e a impraticabilidade de que os auditores independentes emitissem seus pareceres sobre as demonstrações financeiras de forma economicamente viável sem o suporte de um bom sistema de controles internos.

Ainda conforme os autores, em 1977, uma nova legislação norte-americana, denominada *Foreign Corrupt Practices Act*[9] criou a obrigação de atendimento de determinadas práticas contábeis, entre as quais a manutenção de um sistema satisfatório de controles internos.

No entanto, não existia consenso entre gestores, auditores e regulamentadores sobre o que seria um sistema satisfatório de controles internos.

Em 1985, foi criada nos Estados Unidos a *National Commission on* Fraudulent *Financial Reporting*[10] também conhecida como *Treadway Commission*, uma vez que seu responsável principal à época era James C. Treadway, Vice-Presidente Executivo e Advogado Geral de empresa e ex-membro da *Securities and Exchange Commission* (SEC), a Comissão de Valores Mobiliários norte-americana. Tratava-se de uma

[9] Lei das Práticas Anticorrupção Exterior

iniciativa independente criada para estudar as causas da ocorrência de fraudes em relatórios financeiros e contábeis.

Em 1987, essa comissão emitiu um relatório no qual era enfatizada a importância dos controles internos na redução da incidência de relatórios financeiros fraudulentos. Segundo esse documento:

> A mensagem sobre controles internos que a administração passa para o restante da entidade desempenha papel fundamental na prevenção de fraudes financeiras, pois influencia o ambiente corporativo no qual os relatórios financeiros são preparados.
> Todas as companhias abertas deveriam manter controles internos que proporcionassem segurança razoável de que a produção de relatórios financeiros fraudulentos seria impedida ou detectada em estágios iniciais.
> As organizações que patrocinam a Comissão deveriam cooperar no desenvolvimento de diretrizes adicionais sobre sistemas de controles internos (REPORT OF THE NATIONAL COMMISSION ON FRAUDULENT REPORTING, 1987, p.11 apud BOYNTON E OUTROS, 2002, p.320).

As citadas organizações que patrocinavam a Comissão eram cinco das principais associações de profissionais ligados à área financeira nos Estados Unidos, que se auto-intitulavam The Committee of Sponsoring Organizations of the Treadway Commission[11] (COSO). A saber: AICPA, AAA, IIA, Financial Executives Internacional[12] (FEI) e Institute of Management Accountants[13] (IMA).

O COSO foi criado como uma entidade do setor privado, sem fins lucrativos, voltada para o aperfeiçoamento da qualidade de relatórios financeiros por meio de éticas profissionais, implementação de controles internos e governança corporativa. Teve como finalidades iniciais principais o estabelecimento de uma definição comum de controles internos que atendesse à necessidade de diferentes interessados e o fornecimento de um padrão contra o qual empresas e outras entidades – pequenas ou grandes, do setor privado ou público, visando lucro ou não - pudessem avaliar seus sistemas de controles, e determinar como poderiam melhorá-los (COSO, 1992). Para tanto e em atendimento à recomendação do relatório da Comissão Treadway, o COSO publicou em 1992, após três anos de estudos, o documento *Internal Control - Integrated Framework*.

A definição de controles internos existente no Relatório COSO é:

> Controles internos são um processo, conduzido pelo conselho de diretores, por todos os níveis de gerência e por outras pessoas da entidade, projetado para

---

[10] Comissão Nacional sobre Fraudes em Relatórios Financeiros
[11] Comitê das Organizações Patrocinadoras da Comissão Treadway
[12] Executivos Financeiros Internacional
[13] Instituto dos Contadores Gerenciais

> fornecer segurança razoável quanto à consecução de objetivos nas seguintes categorias:
> - eficácia e eficiência das operações;
> - confiabilidade de relatórios financeiros; e
> - cumprimento de leis e regulamentações aplicáveis (COSO, 1992, p. 1,tradução nossa).

É importante a análise dos conceitos fundamentais existentes nessa definição, conforme enfatizado no Relatório. Primeiro, os controles internos são um processo, um meio para se atingir um fim e não um fim em si mesmo. Assim, constituem-se em uma série de ações integradas, e não superpostas, à estrutura da entidade. Segundo, são as pessoas que operam os controles internos, de forma que eles são o resultado da interação de pessoas em todos os níveis da organização, desde os mais altos (conselho de diretores e diretoria) até o quadro de pessoal em geral.

O terceiro conceito se relaciona ao fato de que os controles internos não trazem segurança absoluta, mas apenas segurança razoável ao gerenciamento de uma organização. Isto é, quando eficientes, os controles auxiliam, mas não garantem, a consecução dos objetivos, devido a suas limitações inerentes. Entre as possíveis limitações existentes, pode-se citar: a possibilidade de falhas; erros de julgamentos em decisões; a ocorrência de eventos externos além da ingerência dos administradores; o conluio entre empregados; a sua transgressão por parte da própria administração; e a consideração de custo x benefícios que deve ser feita, uma vez que os controles não podem custar mais do que aquilo que é controlado.

Por fim, os controles internos estão vinculados ao alcance de objetivos nas categorias de elaboração e apresentação de demonstrativos financeiros, conformidade a normas, e desempenho nas operações. Dessa forma, está implícita a idéia de que a administração deve formular e manter atualizados os objetivos da instituição nessas três categorias.

Para o COSO, o processo de controles internos deve ser constituído de cinco componentes, a saber:

> **Ambiente de Controle**: dá o tom de uma organização, influenciando a consciência de controle das pessoas que nela trabalham. Representa o alicerce dos demais componentes, disciplinando-os e estruturando-os.
> **Avaliação de Risco**: identificação e análise dos riscos relevantes para a consecução dos objetivos da entidade; forma a base para a determinação de como os riscos devem ser administrados.
> **Atividades de Controle**: políticas e procedimentos que ajudam a assegurar que as diretrizes da administração estejam sendo seguidas.
> **Informação e Comunicação**: identificação, captura e troca de informações sob forma e em época tais que permitam que as pessoas cumpram suas responsabilidades.

> **Monitoração**: processo que avalia a qualidade do desempenho dos controles internos (INTERNAL CONTROL – INTEGRATED FRAMEWORK – COSO, 1992 apud BOYNTON E OUTROS, 2002, p. 321).

O detalhamento desses componentes, assim como a forma como eles se inter-relacionam, será objeto de aprofundamento de análise posteriormente neste texto, quando for realizada a descrição do novo modelo COSO, "Modelo de Gerenciamento de Risco Empresarial".

Cocurullo (2002, p. 85) comenta sobre a importância do Relatório COSO tanto a nível conceitual como prático. De acordo com o autor, a matriz de análise dos controles internos foi utilizada em diversas situações reais, provendo, em cada caso, não só a base para determinar fraquezas, como a direção para ações corretivas. Ainda, "gerências de várias indústrias abarcaram os conceitos do relatório. Eles reconhecem e apreciam que estes conceitos contribuirão ao longo do tempo para operações mais efetivas e melhoria do gerenciamento corporativo".

2.4 Definição de Riscos

Na seção anterior foi apresentada uma definição de controles internos por parte da INTOSAI, datada de 1986, que servia como síntese das outras definições então apresentadas. Em 1992, a INTOSAI publicou um documento denominado *Guidelines for Internal Control Standards*[14], no qual apresenta uma definição ainda mais genérica, relacionando controles internos a controles gerenciais:

> Controle Interno é uma ferramenta gerencial usada para proporcionar confiança razoável de que os objetivos gerenciais estão sendo atingidos.
> Uma estrutura de controle interno é definida como o plano de organização, incluindo a atitude da gerência, métodos, procedimentos e outras medidas que proporcionam confiança razoável que os seguintes objetivos gerais são atingidos: promoção de operações disciplinadas, econômicas, eficientes e efetivas e produtos e serviços de qualidade consistentes com a missão da organização; salvaguarda de recursos contra perdas devido ao desperdício, uso abusivo, falta de gerenciamento, erros, fraudes e outras irregularidades; aderência a leis, regulamentos e diretrizes gerenciais; e desenvolvimento e manutenção de dados financeiros e gerenciais confiáveis e sua apresentação fidedigna em demonstrações oportunas (INTOSAI, 1992, p.5, tradução nossa).

Mais recentemente, em 2001, essa entidade divulgou um documento que visa a fornecer a gestores e a auditores governamentais um modelo para estabelecer e manter sistemas de controles internos efetivos. Trata-se de uma versão resumida e atualizada do documento de 1992, no qual se encontra, além da conceituação acima citada de controle

[14] Diretrizes para Padrões de Controle Interno

interno, sua relação com a avaliação de riscos seguindo as orientações do Relatório COSO, conforme exposto a seguir:

> Estabelecer controles internos efetivos envolve a avaliação dos riscos que a agência enfrenta tanto de fontes internas como externas. Uma pré-condição para a avaliação de riscos é o estabelecimento de objetivos da entidade claros e consistentes, os quais são as metas ou propósitos a serem alcançados. Avaliação de risco é a identificação e análise dos riscos relevantes associados com o alcance dos objetivos. Práticas de controle interno (tais como procedimentos, processos, estruturação física e organizacional e definição de responsabilidades e autoridades) devem então ser projetadas e implementadas para atingir as metas (INTOSAI, 2001, p. 6, tradução nossa).

Para melhor compreensão do motivo dessas entidades frisarem a necessidade de se avaliar os riscos de um negócio, é importante que se conceitue risco de modo genérico, assim como sua definição particular para a auditoria.

Já há mais de 60 anos, o economista Frank Knight diferenciou incerteza e risco. Para o autor, incerteza refere-se a situações em que uma decisão pode gerar muitos resultados, porém cada um deles apresenta possibilidades de ocorrência desconhecidas. O risco, por sua vez, refere-se a situações para as quais todos os possíveis resultados podem ser relacionados, conhecendo-se a probabilidade de cada resultado ocorrer (Knight apud Rozo).

O que diferencia os dois conceitos é uma maior objetividade inerente ao risco. Quando a tomada de decisões é acompanhada por um desconhecimento dos prováveis efeitos, está-se diante da incerteza. Quando é possível se prever, e aquilatar, as conseqüências, ainda que de modo impreciso quanto à probabilidade e impacto da ocorrência, está-se diante de uma análise de risco. Dessa forma, o risco é algo que pode ser mensurado.

Outro autor, Thompson (1992, p. 13 apud COCURULLO, 2002, p. 50) se referindo especificamente ao risco, o define de forma semelhante, "risco é a variação potencial nos resultados. Está presente em quase tudo o que fazemos. Quando o risco está presente, o resultado não pode ser precisamente previsto". Cocurullo (2002), ao comentar a definição de Thompson frisa a objetividade relacionada ao risco, e sua mensurabilidade.

Outro comentário interessante de Cocurullo (2002) se relaciona ao fato do risco não significar, necessariamente, possibilidade de perda. Assim, ao se determinar o risco, avaliá-lo adequadamente e bem administrá-lo, soluções cautelares apropriadas podem ser previstas, o que, consequentemente, pode gerar resultados benéficos. É o ponto de vista de se enxergar o risco como possibilidade de sucesso e não de fracasso.

Nesse contexto, Bueno (1999 apud COCURULLO, 2002) conceitua o risco como uma medida de probabilidade de perdas possíveis e como desvio-padrão ou volatilidade dos retornos esperados, podendo assumir dois conjuntos de possíveis eventos: os sucessos - eventos que permitem atingir os objetivos; e os fracassos – eventos que não permitem atingir os objetivos.

De uma forma mais direta, risco foi definido pelo COSO (1992) como a possibilidade que um evento ocorra e afete de modo adverso o alcance dos objetivos de uma entidade.

Para definir risco, o TCU buscou aliar conceitos acadêmicos e conceitos mais simples:

> Risco é a expressão da probabilidade de ocorrência e do impacto de eventos futuros incertos que têm potencial para influenciar o alcance dos objetivos de uma organização. Em termos simples e não acadêmicos, risco é todo evento que pode atrapalhar ou impedir que se atinja o alvo pretendido (TCU, 2003, p.3).

Essa conceituação traz embutida a noção de que, para se ter conhecimento dos riscos de uma organização, deve-se primeiro conhecer seus objetivos. A partir daí, busca-se conhecer toda a gama de potenciais eventos passíveis de influenciar o alcance dos objetivos. Se um evento impulsiona o alcance, está-se diante de um sucesso. Se atrapalha ou impede o alcance do objetivo, está-se diante de um fracasso, para se utilizar a conceituação de Bueno. O COSO (2003b), no documento *Enterprise Risk Management Framework*, utiliza os termos oportunidades para representar os sucessos e riscos para representar os fracassos.

Mais, a conceituação fala que se deve tentar estabelecer a probabilidade de ocorrência de um dado evento e, em caso de ocorrência, o impacto para o alcance do objetivo. Portanto, quando se fala que o risco tem caráter objetivo e que pode ser mensurado, pretende-se estabelecer o binômio probabilidade x impacto da ocorrência do evento.

Um dos modelos mais utilizados para se expressar esse binômio é o uso de um gráfico bidimensional com cada uma das variáveis ocupando um eixo (Fig. 1). Dividindo-se o gráfico resultante em quatro quadrantes é possível se criar categorias que, de modo genérico, podem pré-direcionar a ação quanto aos riscos. Para Cocurullo (2003), em caso de riscos de baixa probabilidade de ocorrência e de baixo impacto (1º quadrante), deve-se fazer a seleção de alguns para acompanhamento e verificação de possível migração para outro quadrante. Se os riscos são do 2º quadrante (alto impacto e

baixa probabilidade), devem-se criar planos de contingência e se proteger mediante seguros. Riscos de alta probabilidade de ocorrência, mas de baixo impacto (3º quadrante) devem ser geridos reativamente, isto é, verifica-se a existência e adequabilidade de controles internos para seu gerenciamento. Em caso negativo, esses riscos devem ser tratados como se fossem do 4º quadrante. Esses, dado o alto impacto conjugado com alta probabilidade, devem ser geridos proativamente, isto é devem ser definidas ações de resposta aos riscos (discutidas adiante neste trabalho).

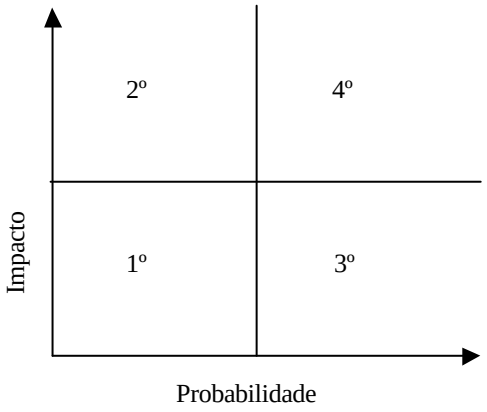


Figura 1 – Expressão bidimensional do binômio probabilidade x impacto

A esse processo sistemático de avaliação de eventos interagindo com os objetivos de uma organização dá-se o nome de análise de risco, conforme a definição do TCU:

> Análise de Risco (AR) é o uso sistemático de informações para identificar os possíveis eventos que podem influenciar o alcance dos objetivos da organização, compreendendo a estimativa da probabilidade de ocorrência do evento e seu impacto potencial na consecução dos alvos organizacionais. É usual dividir a AR em duas áreas: riscos externos (oriundos de eventos cuja ocorrência independe da ação dos gestores) e riscos internos (oriundos das atividades/processos intrínsecos da entidade) (TCU, 2003, p.3).

2.5 Materialidade, Risco de Auditoria e Evidência

Conforme definido, risco é todo evento capaz de atrapalhar ou impedir a consecução de um objetivo. Auditoria foi definida, em um sentido bastante amplo, como “o ato de se confrontar a condição – situação encontrada – com o critério – situação que deve ser” (ARAÚJO, 1998, p. 15). Logo, risco de auditoria pode ser

definido como qualquer evento capaz de atrapalhar ou impedir que o objetivo de auditoria, dar um informe fiel acerca da confrontação critério x situação, seja alcançado.

Como visto, existem diversas definições para auditoria, que variam de acordo com o objeto a que ela se destina. Existem, da mesma forma, variadas conceituações de risco de auditoria. Entre as melhores e mais utilizadas, inclusive por diversos autores, estão aquelas que partem das entidades de classe de contabilidade e auditoria.

A IFAC edita as *International Standards on Auditing*[15] (ISA), que devem ser aplicadas à auditoria de demonstrações contábeis. A ISA 400 se refere à avaliação de riscos e controles internos. Para a norma "risco de auditoria significa o risco de que o auditor dê um parecer de auditoria impróprio, quando as demonstrações contábeis contiverem distorções relevantes" (IFAC, 2001, p.249, tradução nossa). O CFC (1997) e o AICPA (SAS 47 e 82 apud BOYNTON E OUTROS, 2002) definem risco de auditoria de maneira semelhante. Essa definição, voltada para a auditoria de demonstrações financeiras, é coerente com a definição geral apresentada. O objetivo desse tipo de auditoria é a emissão de um parecer sobre a fidedignidade das afirmações da administração feitas nas demonstrações contábeis, e o risco, então, se situa na existência de qualquer fator que faça com que o parecer de auditoria não esteja em sintonia com a realidade contábil-financeira da entidade.

A IFAC e o AICPA dividem o risco de auditoria em três componentes, a saber: risco inerente, risco de controle e risco de detecção.

Antes, porém, de se falar sobre os três componentes do risco de auditoria, é indispensável se comentar rapidamente sobre dois outros conceitos fundamentais para o processo de auditoria: materialidade ou relevância e evidência.

Materialidade ou relevância pode ser definida como qualquer omissão ou erro que, considerando as circunstâncias presentes, torna provável que o julgamento do usuário baseado nas demonstrações financeiras poderia ser alterado ou influenciado por esse erro ou omissão (GOMES, 2003). Essa definição parte do ponto de vista do usuário das demonstrações contábeis, que deve ter uma visão fiel da situação da entidade a partir dessas demonstrações. A questão é que nem todo erro ou omissão presente nas demonstrações é de tal monta que venha a macular a sua fidedignidade. A materialidade, então, representa a análise do grau de influência que um erro ou omissão por parte da administração, constatado pelos procedimentos de auditoria, pode ter sobre

[15] Normas Internacionais de Auditoria

as demonstrações financeiras, ou sobre o objetivo de auditoria, de uma forma geral. Para tanto, deve-se buscar critérios de valor ou quantidade e de natureza ou qualidade, relativizando-os, sempre, às circunstâncias, ao contexto de cada entidade. Assim, o que é material, relevante para certa auditoria, pode não o ser em outra.

Voltando-se a definição de risco de auditoria pela IFAC, vê-se que se define o risco baseado em um critério de relevância, uma vez que, erros ou omissões em contas ou transações não relevantes não implicam risco para obtenção do objetivo de auditoria.

Evidência, de uma forma geral, pode ser entendida como o material necessário (dados financeiros, contábeis, gerenciais, provas documentais, provas testemunhais, entre outros) suficiente (em volume adequado) e competente (confiável) para dar ao auditor conforto quanto à obtenção do objetivo da auditoria. Na realidade, a coleta e a avaliação de evidências representam o ponto central, o próprio objeto da auditoria.

Conforme Boynton e outros (2002, p. 186), "o auditor realiza procedimentos de auditoria para obter evidências que fundamentem seu parecer sobre as demonstrações contábeis". Os autores definem uma categorização dos procedimentos de auditoria, de acordo com seus objetivos, como se segue:

- **procedimentos para obtenção do entendimento do negócio e dos controles internos do auditado**: conforme o próprio nome já diz, representa todas as atividades relacionadas ao conhecimento prévio indispensável à realização da auditoria. Destacam-se: conhecimento dos fatores competitivos da indústria, incluindo as características de melhor desempenho; e conhecimento do negócio do auditado, incluindo seus produtos, processos, sistemas de produção e distribuição e as atividades econômicas subjacentes ao negócio. Trata-se de uma avaliação de risco inerente, que será definido a seguir.

  Uma atividade essencial a ser realizada nessa etapa é o entendimento dos controles internos do auditado. Essa é uma atividade obrigatória para todas as auditorias de demonstrativos contábeis, onde o auditor busca conhecer o desenho da estrutura dos controles internos, isto é, como eles devem funcionar;
- **testes de controle**: visam a confirmação do funcionamento dos controles internos conforme planejados, além de sua eficácia. Não são obrigatórios, mas bastante desejáveis, para se obter uma visão adequada do risco de controle, também, a seguir definido; e

- **testes substantivos:** fornecem as evidências das adequações das afirmações da administração nas demonstrações contábeis, ou, de uma forma mais ampla, trata-se da própria coleta de informações que irão balizar os objetivos de auditoria. São subdivididos em;
  - **procedimentos de revisão analítica:** envolvem a utilização de comparações para se avaliar a adequação de certa informação;
  - **testes de detalhes de transação:** são o exame da documentação relacionada a uma certa transação ou processo; e
  - **testes de detalhes de saldos:** envolvem o exame da fundamentação do saldo final de uma conta contábil.

Há uma relação imediata entre relevância e a obtenção de evidências. Geralmente quanto maior o nível de materialidade de certa conta ou transação para a auditoria, maior o volume necessário de evidências, isto é, maior a necessidade de realização de testes para que o auditor se sinta satisfeito. Aqui, entra também o conceito de risco de auditoria, uma vez que quanto maior o risco envolvido em uma auditoria, maior a necessidade de realização de testes, quer dizer maior volume necessário de evidências para se alcançar a satisfação do auditor. A maneira como se define o nível do risco de auditoria está relacionada com os seus três componentes, a seguir definidos.

O risco de auditoria apresenta três componentes: risco inerente; risco de controle; e risco de detecção. Apresenta-se a definição do AICPA, frisando que o IFAC relaciona os três conceitos de maneira assemelhada. O risco inerente é definido como a "suscetibilidade de uma afirmação a um erro ou classificação indevida material, supondo que não haja controles" (AICPA apud BOYNTON E OUTROS, 2002, p. 293). De acordo com Houaiss (2001), inerente significa algo que só existe em relação a um sujeito, a uma maneira de ser que é intrínseca a esse. Então, risco inerente, em uma concepção mais abrangente, é aquele que considera os riscos do negócio, riscos que nascem com as atividades desenvolvidas pela entidade e se mantêm os mesmos caso não existam controles internos para mitigá-los.

O Modelo de Gerenciamento de Riscos Empresariais do COSO, objeto primordial de estudo deste texto, é um modelo que visa a entender, avaliar e gerenciar os riscos inerentes de uma entidade.

Mesmo com a existência de controles internos, inclusive a auditoria interna, há a possibilidade de que eles possam falhar na prevenção ou detecção, em tempo hábil, de

erros, omissões ou irregularidades materiais. Ainda, os controles podem existir, mas serem mal planejados, de modo que, também, não identifiquem falhas. Surge daí, o risco de controle, que é definido pelo AICPA (AICPA apud BOYNTON E OUTROS, 2002, p. 295) como "o risco de que um erro ou classificação indevida de materialidade que possam constar de uma afirmação não sejam evitados ou detectados tempestivamente pelos controles internos da entidade".

Uma característica importante do risco de controle é que ele nunca pode ser considerado nulo, porque os controles internos não conseguem fornecer, por melhor que sejam, confiança total na detecção e correção de erros, omissões e irregularidades.

Tanto o risco inerente, como o risco de controle são independentes da ação do auditor em uma dada auditoria. É claro que a ação do auditor mediante recomendações, ou mesmo determinações como no caso do TCU, pode alterar a forma como os riscos inerentes são tratados pela entidade, assim como melhorar a condição dos controles internos, vindo a diminuir os riscos associados. No entanto, quando se considera o planejamento de uma auditoria específica, a ação do auditor refere-se, somente, a melhorar o nível de avaliação que ele pode fazer dos citados riscos. Assim, a busca mais acentuada de evidências relacionadas aos "procedimentos para obtenção do conhecimento do negócio" e aos "testes de controle" podem gerar um nível mais acurado na definição dos riscos inerente e de controle.

O último componente do risco de auditoria é o risco de detecção. É definido pelo AICPA (AICPA apud BOYNTON E OUTROS, 2002, p. 297) como "o risco de que o auditor não detecte um erro ou classificação indevida relevante que existe em uma afirmação". Assim, o risco de detecção é aquele relacionado ao próprio trabalho do auditor, à possibilidade de que os testes substantivos aplicados não detectem erros, omissões ou irregularidades existentes.

Pela própria definição, verifica-se que esse risco está sujeito à ingerência do auditor, de forma que um risco de detecção mais baixo pode ser obtido pela utilização de procedimentos de auditoria mais eficazes, pela realização de um maior número de testes substantivos, assim como pela utilização de uma equipe de auditoria com mais experiência profissional. Outro fator importante é a possibilidade de erro na ação do auditor, que é assim tratada por Boynton e outros:

> Ao determinar o risco de detecção o auditor deve também considerar a probabilidade de que ele venha a cometer um erro – aplicando erroneamente um procedimento de auditoria ou interpretando inadequadamente uma evidência constatada, por exemplo. Esses aspectos do risco de detecção podem

> ser reduzidos mediante planejamento e supervisão adequados, e obediência às normas de controle e qualidade (BOYNTON E OUTROS, 2002, p. 297).

Definidos esses três componentes, deve-se entender como eles se relacionam para criar o risco de auditoria. O risco de auditoria é uma escolha do auditor, que traduz o nível de confiança que o seu trabalho de auditoria trará para o interessado. Aqui se introduz mais um conceito, o de confiança, que reflete a garantia dada pelo auditor do grau de certeza de suas afirmações. Assim, ao definir um risco de auditoria de 5%, o auditor está dizendo ao interessado em seu trabalho que suas afirmações possuem um nível de confiança de 95%, isto é, há 95% de probabilidade de que suas afirmações estejam corretas.

Basicamente, os riscos podem ser definidos de uma forma quantitativa (mediante percentuais, por exemplo) ou qualitativa (alto, médio ou baixo, por exemplo). Se o tratamento dado for quantitativo, o modelo do risco de auditoria segue uma expressão matemática, na qual o risco de auditoria (RA) é a resultante da multiplicação do risco inerente (RI), risco de controle (RC) e risco de detecção (RD), conforme a seguir:

$$RA = RI \times RC \times RD$$

Como exemplo, considere-se a situação descrita de um risco de auditoria desejado de 5%. Supondo-se que o auditor após a realização de testes, avaliou um risco inerente de 80% e um risco de controle de 50%, o risco de detecção será de:

$$RD = RA / (RI \times RC) = 0,05 / (0,8 \times 0,5) = 12,50\%$$

Como a confiança é o valor complementar do risco de detecção (1- 0,125), a confiança necessária para os testes substantivos deve ser de 87,5%, isto é o auditor deve planejar testes substantivos tais que a probabilidade de que eles não detectem erros, omissões ou irregularidades existentes seja de 12,5%.

Para uma opção qualitativa do tratamento dos riscos, a IFAC apresenta, no apêndice da citada norma ISA 400, uma tabela, reproduzida a seguir, que mostra que o nível aceitável de risco de detecção (área cinzenta) varia inversamente à combinação das avaliações dos riscos inerente e de controle, para que o risco de auditoria se mantenha sempre em nível baixo. Esse tipo de abordagem é consistente com o modelo matemático apresentado, no qual o risco de detecção também varia inversamente com a combinação dos dois outros riscos.

Tabela 1 – Risco de Detecção em função dos Riscos Inerente e de Controle – Avaliação Qualitativa

		A avaliação do risco de controle pelo auditor é:		
		Alto	Médio	Baixo
A avaliação do risco inerente pelo auditor é:	Alto	Menor	Menor	Médio
	Médio	Menor	Médio	Maior
	Baixo	Médio	Maior	Maior

Fonte: IFAC, 2001, p.261

Na ISA 400, o IFAC define qual deve ser, em grandes modos, o procedimento do auditor quanto ao risco de auditoria:

> Ao desenvolver a abordagem de auditoria, o auditor considera a avaliação preliminar de risco de controle (em conjunto com a avaliação de risco inerente), para determinar qual seja o risco de detecção apropriado a aceitar para as asserções contidas nas demonstrações contábeis e também para determinar a natureza, época de aplicação e extensão dos procedimentos de comprovação de tais asserções (IFAC, 2001, p. 251, tradução nossa).

Conforme visto, os riscos inerente e de controle são avaliados pelo auditor em uma dada auditoria, não podendo por ele ser alterados, visto serem relativos à entidade auditada.

Vistos o conceito e a importância de risco de auditoria e de seus três componentes, deve-se comentar que o TCU não define explicitamente esses três componentes em nenhuma documentação própria acerca de auditoria. Assim, reproduz-se, a seguir, inclusive como sugestão para adoção interna, o conceito de risco de auditoria e de seus três componentes expresso pelo Tribunal de Contas Europeu, no documento Políticas e Normas de Auditoria do Tribunal:

> Risco de Auditoria: É o risco de que o Tribunal expresse uma opinião segundo a qual as contas são fiáveis quando na realidade não o são, as operações subjacentes são legais e regulares quando tal não se verifica, ou houve uma boa gestão financeira quando isso não é verdade (TRIBUNAL DE CONTAS EUROPEU, 2002, p. 10)
> Risco Inerente: É o risco, relacionado com a natureza das atividades, operações e estruturas de gestão, de ocorrência de erros ou deficiências na gestão financeira que, caso não sejam evitados ou detectados e corrigidos pelos procedimentos de controle interno, façam com que as contas não sejam fiáveis, que as operações subjacentes sejam em larga medida ilegais ou irregulares ou provoquem uma má gestão financeira (TRIBUNAL DE CONTAS EUROPEU, 2002, p. 10).
> Risco de Controle: É o risco de que os procedimentos de controle interno não evitem ou não detectem e corrijam em tempo oportuno erros ou deficiências significativos da gestão financeira (TRIBUNAL DE CONTAS EUROPEU, 2002, p. 10).
> Risco de Detecção: É o risco de que os procedimentos substantivos aplicados pelo auditor não permitam detectar um erro ou uma deficiência da gestão

> financeira que, isolados ou acumulados com outros erros ou deficiências, possam ser significativos (TRIBUNAL DE CONTAS EUROPEU, 2002, p. 12).

Essas definições são totalmente coerentes com as anteriormente apresentadas, e exprimem situações de trabalho mais próximas com o trabalho desenvolvido pelo TCU. Assim, fala-se em expressão de opinião relativa a contas, a operações legais e regulares (conformidade) e a boa gestão financeira (operacional).

2.6 Gerenciamento de Risco

Anteriormente foi expresso neste texto o conceito de análise de risco. No entanto, evidentemente, não basta a uma entidade poder identificar os riscos a que está sujeita. É necessária a existência de uma ação sistêmica para tratar esses riscos identificados de modo que os objetivos possam ser alcançados. A essa ação sistêmica dá-se o nome de gerenciamento de risco, que na definição do TCU é:

> Um método sistemático de identificar, analisar, avaliar, tratar, monitorar e comunicar riscos, a fim de manter o grau de exposição da organização a riscos em nível aceitável. Em princípio, pode-se gerenciar riscos buscando reduzir a possibilidade de ocorrência do evento indesejado ou minimizando-se o impacto sobre os objetivos (TCU, 2003, p. 3).

Um conceito importante que se extrai dessa definição é que, usualmente, as ações que envolvem o gerenciamento de risco não conseguem eliminar completamente um risco, devendo, no entanto, fazer com que a probabilidade de sua ocorrência seja diminuída e, no caso de ocorrência, o impacto seja minimizado. Nesse sentido, manifestam-se Cicco e Fantazini (1985, p. 15, apud COCURULLO, 2002, p. 75) que definem a gerência de riscos como um processo de planejamento, orientação e controle dos recursos e atividades, que busca minimizar conseqüências adversas, em uma organização, ao menor custo possível.

O COSO exprime a relevância do gerenciamento do risco empresarial já no início do documento *Enterprise Risk Management Framework*. Para a entidade:

> A premissa implícita no gerenciamento do risco empresarial é que toda entidade, seja ela lucrativa, não-lucrativa ou pertencente ao governo, existe para prover valor a seus grupos interessados. Todas as entidades enfrentam incerteza, e o desafio da gerência é determinar quanta incerteza a entidade está preparada para aceitar na sua tentativa de crescer o valor provido a seus grupos interessados. A incerteza significa tanto riscos quanto oportunidades, com o potencial de corroer ou incrementar o valor. O gerenciamento de risco empresarial fornece um modelo para que a gerência efetivamente lide com a incerteza e os seus riscos e oportunidades associados e, mediante isso, aumente sua capacidade de produzir valor (COSO, 2003b, p. 1, tradução nossa).

A incerteza decorre da inabilidade de precisamente se determinar a possibilidade de ocorrência de eventos e suas conseqüências associadas, relacionando-se, também, às escolhas estratégicas feitas pelas entidades. Já a criação de valor é reconhecida diferentemente por distintos grupos de interessados. Para companhias, está relacionado ao crescimento do valor das ações. Para entidades governamentais, o valor é provido quando os eleitores reconhecem o recebimento de serviços a custos aceitáveis. Para entidades não lucrativas, o valor se relaciona à recepção de benefícios sociais. O gerenciamento de riscos proporcionaria habilidade aos gerentes tanto para criar valor sustentável, quanto para comunicar a criação de valor aos grupos interessados (COSO, 2003b, p.1, tradução nossa).

É interessante notar a diferença de conceituação apresentada quanto à incerteza e ao risco e quanto às definições apresentadas anteriormente neste texto. Para o COSO a incerteza, que advém da dificuldade de se prever precisamente eventos e suas conseqüências, pode significar tanto riscos, quando corrói o valor, quanto oportunidades, quando o incrementa. Anteriormente, relacionou-se a incerteza com o desconhecimento dos prováveis efeitos da tomada de decisões, e o risco a uma probabilidade, ainda que imprecisa, de previsão. Os riscos seriam classificados em sucessos ou fracassos, de acordo com as conseqüências advindas. No entanto, a despeito da certa diferença de conceituação, o que realmente importa é a noção de que existem eventos que podem impossibilitar ou incrementar o alcance dos objetivos de uma entidade, e que esses eventos devem ser identificados, avaliados, tratados, monitorados e comunicados, conforme a definição apresentada pelo TCU.

Ao discorrer sobre os benefícios do gerenciamento de risco, o COSO frisa que nenhuma empresa opera em um ambiente sem riscos, e que o gerenciamento de riscos não cria tal ambiente, mas que cria condições para que o gerente opere mais eficientemente em um ambiente cheio de riscos. Para a entidade, o gerenciamento de riscos apresenta uma série de benefícios listados a seguir (COSO, 2003b, p.2, tradução nossa):

- provê o alinhamento do apetite ao risco e da estratégia. O apetite ao risco é definido como o grau de risco, em um nível amplo, que a entidade está disposta a correr no alcance de seus objetivos. Assim, a gerência deveria considerar seu apetite ao risco, inicialmente, ao avaliar suas alternativas

estratégicas, ao definir os objetivos alinhados às estratégias e ao desenvolver mecanismos para controlar os riscos relacionados;

- une crescimento, risco e retorno por proporcionar uma habilidade desenvolvida para identificar e avaliar riscos, e estabelecer níveis aceitáveis de risco relacionados aos objetivos de crescimento e retorno;
- incrementa as decisões de resposta ao risco, uma vez que cria o rigor necessário para identificar e selecionar entre as respostas ao risco possíveis (explicadas com mais detalhes adiante): fuga, redução, compartilhamento e aceitação;
- minimiza perdas e surpresas operacionais, devido ao aumento da capacidade de identificar eventos potenciais e suas conseqüências;
- identifica e gerencia riscos cruzados existentes dentro das várias áreas de uma empresa, dada a necessidade de se conhecer os impactos inter-relacionados dos eventos;
- provê respostas integradas a múltiplos riscos, efeito relacionado ao benefício anterior;
- aproveita oportunidades, pois ao analisar um ampla gama de eventos potenciais, a gerência acaba por identificar eventos que significam oportunidades, e não riscos;
- aumenta a racionalização na definição do capital total necessário, assim como na sua alocação, devido ao maior conhecimento dos riscos e das necessidades.

Embora o modelo conceitual de gerenciamento de risco proposto pelo COSO seja essencialmente destinado a empresas privadas, os benefícios advindos desse processo de gerenciamento podem claramente ser percebidos para todo tipo de organização, inclusive governamentais que não visem o lucro, mas benefícios sociais. Na realidade, o que importa é a existência de objetivos e a busca da entidade para alcançá-los. Essa idéia é bem retratada nos textos a seguir:

> Gerenciamento de risco empresarial não é um fim em si mesmo, mas, na verdade, um importante meio das entidades atingirem seus objetivos. Ele não funciona isoladamente, se constituindo em um capacitador do processo de gerenciamento. Ele se inter-relaciona com governança corporativa[16], ao prover

[16] Governança corporativa são as práticas e os relacionamentos entre os Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal, com a finalidade de otimizar o desempenho da empresa e facilitar o acesso ao capital.

> informação à diretoria sobre os riscos mais significativos e como eles estão sendo gerenciados. E ele se inter-relaciona com gerenciamento de desempenho ao prover medidas de ajuste ao risco, e com o controle interno, que é parte integrante do gerenciamento de risco empresarial (COSO, 2003b, p. 4, tradução nossa).
>
> O gerenciamento de risco empresarial ajuda uma entidade a alcançar seus alvos de desempenho e lucratividade e a prevenir a perda de recursos. Ajuda a garantir divulgação efetiva. E ajuda a garantir o cumprimento de leis e regulamentações, evitando prejuízo na reputação e outras conseqüências. Em suma, ajuda uma entidade a chegar aonde deseja e evitar armadilhas e surpresas ao longo do caminho (COSO, 2003b, p. 5, tradução nossa).

A expressão é designada para abranger os assuntos relativos ao poder de controle e direção de uma empresa, bem como as diferentes formas e esferas de seu exercício e os diversos interesses que, de alguma forma, estão ligados à vida das sociedades comerciais.

Na teoria econômica tradicional, a governança corporativa surge para procurar superar o chamado "conflito de agência", presente a partir do fenômeno da separação entre a propriedade e a gestão empresarial. O "principal", titular da propriedade, delega ao "agente" o poder de decisão sobre essa propriedade. A partir daí surgem os chamados conflitos de agência, pois os interesses daquele que administra a propriedade nem sempre estão alinhados com os de seu titular. Sob a perspectiva da teoria da agência, a preocupação maior é criar mecanismos eficientes (sistemas de monitoramento e incentivos) para garantir que o comportamento dos executivos esteja alinhado com o interesse dos acionistas.

A boa governança corporativa proporciona aos proprietários (acionistas ou cotistas) a gestão estratégica de sua empresa e a efetiva monitoração da direção executiva. As principais ferramentas que asseguram o controle da propriedade sobre a gestão são o Conselho de Administração, a Auditoria Independente e o Conselho Fiscal.

A empresa que opta pelas boas práticas de governança corporativa adota como linhas mestras transparência, prestação de contas (accountability) e eqüidade. Para que essa tríade esteja presente em suas diretrizes de governo, é necessário que o Conselho de Administração, representante dos proprietários do capital (acionistas ou cotistas), exerça seu papel na organização, que consiste especialmente em estabelecer estratégias para a empresa, eleger a Diretoria, fiscalizar e avaliar o desempenho da gestão e escolher a auditoria independente. (disponível em <http://www.ibgc.org.br>. Acesso em 29/dez/2003). IBGC é a sigla do Instituto Brasileiro de Governança Corporativa.

3. Exposição da Metodologia de Gerenciamento de Risco Empresarial (*Enterprise Risk Management Framework)* do COSO

A idéia deste Capítulo é apresentar a Metodologia de Gerenciamento de Risco Empresarial, conforme definida pelo COSO no documento *Enterprise Risk Management Framework* (COSO, 2003b). Os conceitos expressos foram todos retirados do citado documento.

O objetivo primordial da metodologia é ajudar gerentes de organizações a melhor lidar com os riscos inerentes ao alcance de seus objetivos. Para tanto, integra vários conceitos de gerenciamento de risco em um modelo único, no qual definições comuns são estabelecidas e componentes identificados.

Inicialmente, estabelece-se que uma infinidade de eventos, de fontes internas e externas, têm o potencial de afetar a execução de estratégias e o alcance de objetivos. Tais eventos podem ter um impacto negativo, positivo, ou ambos. Define-se risco como a possibilidade de que um evento ocorra e afete negativamente o alcance de objetivos. Eventos com efeitos positivos representam oportunidades.

Para a entidade:

> Gerenciamento de Risco Empresarial é um processo, efetuado pela diretoria da entidade, sua gerência e outras pessoas, aplicado na definição das estratégias e através da empresa, projetado para identificar eventos potenciais que podem afetar a entidade e conduzir os riscos dentro do apetite ao risco, e para prover um nível razoável de segurança com respeito ao alcance dos objetivos da entidade (COSO, 2003b, p. 6, tradução nossa).

A definição é ampla por capturar conceitos chaves fundamentais sobre como companhias e outras organizações gerenciam risco, provendo uma base para aplicação em diferentes tipos de indústrias, setores e organizações.

Estendendo os conceitos da definição tem-se:

Um Processo, significando que o gerenciamento de risco não é um evento ou circunstância, mas uma série de ações que permeiam as atividades de uma entidade. Essas ações são difundidas e inerentes à forma com que os negócios são gerenciados, sendo mais efetivas quando construídas dentro da infra-estrutura da entidade, sendo parte de sua essência.

Efetuado por Pessoas, uma vez que são elas que definem a missão, a visão, a estratégia e os objetivos de uma entidade e colocam o gerenciamento de risco em funcionamento, afetando esses processos e tendo suas atividades diárias por ele afetadas. Dado que cada pessoa tem um ponto de referência próprio, que influencia

como ela identifica, avalia e responde a riscos, o modelo de gerenciamento de riscos proporciona o mecanismo necessário para que elas entendam risco no contexto dos objetivos da entidade.

Aplicado na Definição das Estratégias. Uma entidade define sua missão, sua visão e estabelece objetivos estratégicos, os quais são metas de alto nível que se alinham e dão suporte à missão e à visão. Estabelece uma estratégia para alcançar tais objetivos, além de determinar objetivos mais focados que deseja atingir, que se distribuem entre as unidades de negócio, divisões e processos da entidade. O gerenciamento de risco é aplicado na definição da estratégia e objetivos estratégicos da entidade.

Aplicado através da Empresa. Para que o gerenciamento de risco seja eficientemente aplicado, há que se considerar todo o escopo de atividades da empresa, criando-se uma visão sistêmica de risco. A partir da visão de risco de cada unidade, desenvolvida, possivelmente, pelos responsáveis de cada área, o gerente geral da área de risco determina se o risco total da empresa se alinha com o apetite ao risco.

Apetite ao Risco. O apetite ao risco é o montante de risco que uma entidade aceita correr na sua busca por produção de valor. Está diretamente relacionado à estratégia empresarial, uma vez que diferentes estratégias irão expor a empresa a diferentes riscos, que devem estar alinhados ao apetite ao risco.

Provê um Nível Razoável de Segurança. A falta de certeza absoluta no gerenciamento de risco reflete o fato de ele se referir ao futuro. Outras limitações envolvem: a possibilidade de julgamentos errados; a necessidade de consideração da relação custo x benefício na definição de ações em resposta a riscos e controles internos; a ocorrência de acidentes devido a erros humanos; o conluio entre duas ou mais pessoas para frustrar controles; e o fato de que a própria gerência da empresa tem, por vezes, a capacidade de se sobrepujar ao que é definido pelo gerenciamento de risco. Essas limitações impedem que se tenha segurança absoluta de que os objetivos da entidade serão alcançados.

Alcance dos Objetivos. Como risco é definido como a possibilidade de ocorrência de eventos que impeçam a consecução dos objetivos, ogerenciamento de risco visa, em última instância, a incrementar a possibilidade de melhores escolhas pelos gerentes. Busca-se prover, tanto gerentes locais como a alta gerência, de mecanismos que os conscientize, em tempo hábil, dos caminhos que a entidade está tomando na direção da consecução de seus objetivos.

Para tanto, o modelo de gerenciamento de risco visualiza os objetivos de uma entidade em quatro categorias:

1. estratégicos: relativos a metas de alto nível, alinhados e dando suporte à missão da entidade;
2. operacionais: relativos à efetividade e à eficiência do uso dos recursos da entidade;
3. de divulgação: relativos à confiança quanto à divulgação de informações pela entidade;
4. de conformidade: relativos à conformidade às leis e aos regulamentos aplicáveis às operações da entidade.

O modelo de gerenciamento de risco empresarial do COSO é composto por oito componentes inter-relacionados, que, de forma resumida, podem ser assim expressos:

1. ambiente interno: define a forma pela qual risco e controle são vistos e comunicados pelas pessoas de uma entidade. Reflete o fato de que as pessoas, seus atributos individuais como integridade, valores éticos e competência, e a forma como elas se relacionam são o coração de qualquer negócio;
2. definição de objetivos: a explicitação de objetivos, que sustentem a visão e missão da entidade, deve existir antes que o gerenciamento de riscos possa identificar eventos que potencialmente impeçam sua consecução;
3. identificação de eventos: inclui a identificação de fatores, internos e externos, que influenciam como os eventos potenciais podem afetar a implementação da estratégia e o alcance dos objetivos. Os eventos são classificados como riscos ou oportunidades, se constituírem barreiras ou impulsos ao alcance dos objetivos;
4. avaliação de riscos: os riscos identificados são analisados para formar uma base de como devem ser administrados;
5. resposta ao risco: selecionam-se formas de atuação de como alinhar os riscos identificados ao apetite ao risco, no contexto dos objetivos estratégicos. São identificadas e avaliadas possíveis respostas aos riscos, as quais incluem: evitar; aceitar; reduzir ou dividir os riscos;
6. atividades de controle: políticas e procedimentos são estabelecidos e executados para ajudar a garantir que as respostas ao risco selecionadas são efetivamente executadas;

7. informação e comunicação: as pessoas devem receber informação clara sobre suas atribuições e responsabilidades. Devem existir meios para que a informação relevante seja identificada, capturada e comunicada de forma a prover condições para que as pessoas exerçam suas responsabilidades. Como a informação em todos os níveis da entidade é fundamental para a avaliação e resposta aos riscos, a comunicação efetiva deve ocorrer em nível amplo, fluindo para baixo, através e para cima da entidade;
8. monitoramento: todos os processos de gerenciamento de risco da entidade devem ser monitorados, de forma que as modificações necessárias ocorram em tempo hábil. O monitoramento pode ocorrer tanto em conjunto com atividades de gerenciamento, quanto mediante avaliações pontuais, ou, ainda, pela combinação de ambos.

Uma importante questão levantada é que o gerenciamento de risco não é um modelo pronto, acabado, que será implantado da mesma forma por todas as entidades. O documento destaca que a intensidade do uso de cada um dos oito componentes do modelo dependerá da indústria envolvida, do tamanho da entidade e da cultura e filosofia de gerenciamento. Mas, apesar das diferenças de implementação, todos os oito componentes são indispensáveis, e deverão, necessariamente, estar presentes. Assim, a medida da efetividade do gerenciamento de risco em uma empresa, apesar de ser um julgamento subjetivo, deve resultar de uma avaliação da existência e do funcionamento adequado dos oito componentes do modelo.

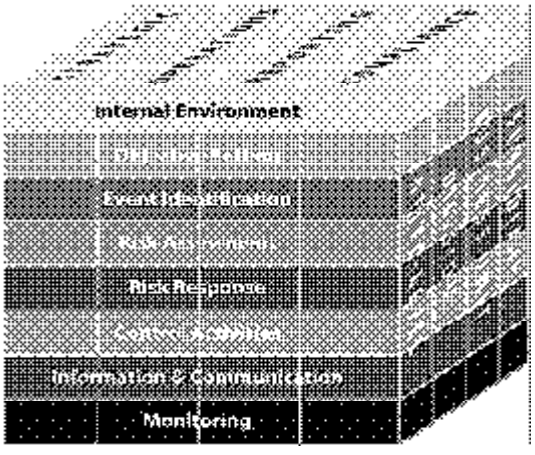


Fig. 2 – Cubo COSO

A figura 2, extraída diretamente do documento em análise, é denominada “Cubo COSO”. Ela representa uma demonstração gráfica da relação direta entre os objetivos

de uma entidade, que representam aquilo que ela pretende alcançar, e os componentes do modelo de avaliação de risco empresarial, que representam aquilo que é necessário para o alcance dos objetivos. As quatro categorias de objetivos são representadas nas colunas verticais, os oito componentes do modelo nas linhas horizontais, e as unidades componentes da entidade na terceira dimensão da matriz.

Como se pode observar da figura, cada componente do modelo se relaciona com todas as categorias de objetivo da entidade. Por exemplo, dados financeiros e não-financeiros gerados por fontes internas e externas, que fazem parte do componente de informação e comunicação ("information and communication"), são necessários na definição de estratégias ("strategic"), no gerenciamento efetivo de operações comerciais ("operations"), na divulgação de informações ("reporting") e na determinação de conformidade com as leis aplicáveis ("compliance").

Da mesma forma, todos os oito componentes do modelo são relevantes para as categorias de objetivo. Por exemplo, todos os oito são aplicáveis e importantes para a efetividade e eficiência das operações.

A terceira dimensão do cubo COSO representa o fato de que o gerenciamento de risco é relevante, e deve ser aplicado na sua totalidade, tanto para a entidade como um todo como para cada unidade de negócio vista de modo individual, para cada divisão ou para cada empresa subsidiária.

Uma importante questão refere-se ao fato de que o sistema de controles internos é uma parte integrante do gerenciamento de risco empresarial, o qual se constitui em uma conceituação e uma ferramenta gerencial mais robusta. O sistema de controles internos é definido e descrito no documento COSO *Internal Control – Integrated Framework*. Uma vez que esse documento é a base para regras, regulamentos e leis existentes, ele foi mantido como a definição e modelo para controles internos, sendo incorporado como referência ao "Modelo para Gerenciamento de Riscos Empresariais".

Uma diferenciação fundamental a ser feita é entre o gerenciamento de risco e o processo de gerenciamento de uma empresa. A esse respeito, o relatório COSO assim se pronuncia:

> Uma vez que o gerenciamento de risco empresarial é parte do processo de gerenciamento, o modelo de gerenciamento de risco empresarial é discutido no contexto daquilo que um gerente faz para dirigir um negócio. Nem tudo que um gerente faz, no entanto, é elemento do gerenciamento de risco. Por exemplo, o processo de estabelecer objetivos é uma parte crítica do gerenciamento de risco, mas a seleção de objetivos específicos, mesmo sendo uma importante responsabilidade gerencial e tendo um importante elo com a estratégia da entidade, não faz parte do gerenciamento de risco. Da mesma

> forma, a etapa de definição de resposta aos riscos, baseada na avaliação dos riscos, é parte do gerenciamento de risco, mas não a escolha de qual específica resposta ao risco a ser usada. Essas são matérias de julgamento de negócios, aplicadas no processo de decisão, entre diversas outras decisões e ações que não são parte do gerenciamento de risco (COSO, 2003b, p. 17, tradução nossa).[17]

[17] Esta diferenciação formulada é fundamental para o entendimento da atividade de auditar o gerenciamento de risco. A ação do TCU deve sempre se pautar pela verificação da existência, e do efetivo funcionamento, de um sistema de gerenciamento de risco nas entidades. No entanto, não cabe ao Tribunal questionar atividades tipicamente gerenciais, tais como a escolha de respostas aos riscos.

A partir de agora serão apresentados em detalhes os oito componentes do "Modelo de Gerenciamento de Risco Operacional" do COSO.

3.1 **Ambiente Interno**

O ambiente interno é a base de todos os outros componentes do gerenciamento de risco, influenciando decisivamente como cada um é estruturado e realizado.

Os elementos a seguir expostos devem ser objeto de consideração quando se analisa o ambiente interno de uma entidade.

Filosofia de Gerenciamento de Risco

Significa as crenças da entidade acerca de risco e como ela escolhe conduzir suas atividades e lidar com riscos. É espelho do que o "topo" da entidade acredita, refletindo-se nas políticas estabelecidas e em outras formas de comunicação. No entanto, não deve ser objeto meramente de palavras, mas de atitudes do dia-a-dia.

Apetite ao Risco

O apetite ao risco é o montante de risco que uma entidade aceita correr na sua busca por produção de valor. Está diretamente relacionado à estratégia empresarial, uma vez que diferentes estratégias irão expor a empresa a diferentes riscos, que devem estar alinhados ao apetite ao risco.

Normalmente é classificado de forma qualitativa em categorias como alto, moderado ou baixo. Pode, também, ser encarado quantitativamente, refletindo metas de crescimento, retorno e risco.

Cultura de Risco

É o conjunto de atitudes, valores e práticas compartilhadas que caracterizam como uma entidade considera o risco nas suas atividades diárias. Nas companhias em que a filosofia de gerenciamento de risco e o apetite ao risco são estabelecidos de forma formal, com comunicação apropriada, a cultura de risco tende a ser homogênea. Na ausência desse comprometimento do topo, tendem a existir diversas culturas de risco fluindo através da entidade.

A existência de diversas "culturas de risco" deve ser tratada pelo gerenciamento de risco, possivelmente repensando a forma como são divulgados a filosofia de gerenciamento de risco e o apetite ao risco, ou mesmo toda a estrutura de gerenciamento de risco empregada.

Um exemplo de como tratar os três elementos até agora definidos é apresentado:

> Uma companhia de gasoduto imaginou uma cultura de risco onde todo o pessoal explicitamente considerasse risco nas suas atividades diárias. Para tanto, um passo foi adicionar uma série de questões focadas em risco nos crachás dos empregados. Essas questões guiavam o seu processo de decisão: "Quais são os riscos? Quem mais pode ser afetado por essa ocorrência? Quem mais precisa ser informado?" As questões encorajavam os empregados a considerar o impacto dos eventos potenciais nas outras unidades e na organização como um todo (COSO, 2003b, p. 20, tradução nossa).

Subculturas de Risco

São as pequenas diferenças de cultura de risco que podem existir entre unidades, funções e departamentos de uma organização, dado ao fato da personalidade do gerente de cada área influenciar como o risco é visto no âmbito de sua gerência. É importante que essas pequenas diferenças (como, por exemplo, uma maior ou menor propensão a correr riscos) sejam tratadas, de forma a refletirem, no conjunto, a filosofia de risco e o apetite ao risco da entidade.

Reconhecimento da Realidade de Risco

Reflete a dificuldade que uma organização que nunca sofreu problemas e perdas significativos tem de reconhecer a existência de riscos. No entanto, é importante que os gerentes entendam que mesmo as entidade bem gerenciadas, com empregados competentes, processos efetivos e tecnologias confiáveis, são sujeitas a riscos, uma vez que as características ambientais internas e externas podem se alterar rapidamente.

Conselho de Diretores[18]

É considerado uma parte crítica, influenciando significativamente todos os outros elementos do ambiente interno. Deve possuir independência do corpo de diretores da empresa e membros com experiência e estatura. Deve ser composto por pessoas com um grau apropriado de conhecimento técnico de gerenciamento e do ramo de atividade da empresa. Uma vez que deve estar hábil a questionar as atividades da gerência e apresentar caminhos de ação alternativos, deve incluir membros externos à direção, e membros da direção, que tragam o conhecimento do dia-a-dia. No entanto, no intuito de se manter a independência necessária, os membros externos devem constituir a maioria.

Deve-se analisar o seu grau de comprometimento com as atividades estratégicas na empresa e o quanto que suas decisões são seguidas pela diretoria, além do nível de interação com o comitê de auditoria, se existente, e com as auditorias interna e externa.

[18] O termo usado no texto, conselho de diretores, pode ser entendido em empresas brasileiras como o Conselho de Administração definido pela Lei das S.A.

Integridade e Valores Éticos

A execução das estratégias e o alcance dos objetivos de uma entidade são baseados em preferências, julgamento de valores e estilo de gerenciamento. A integridade da gerência e o compromisso com valores éticos influenciam essas preferências e julgamentos de valores, traduzindo-os em padrões de comportamento.

A cultura de uma corporação é fortemente influenciada pelos padrões éticos de comportamento e de gerenciamento existentes, pela forma como eles são comunicados e reforçados. Políticas oficiais especificam o que a alta gerência quer que ocorra, mas é a cultura da empresa que determina o que realmente ocorre, quais regras são respeitadas, contornadas ou ignoradas. E a alta gerência, iniciando pelo presidente ou diretor principal, tem um papel preponderante na determinação da cultura corporativa. É ele quem, normalmente, define o tom ético da organização.

A integridade da gerência é pré-requisito para um comportamento ético em todos os aspectos das atividades de uma entidade. A efetividade do gerenciamento de risco está diretamente relacionada à integridade e aos valores éticos de quem cria, administra e monitora tais atividades.

Outros fatores organizacionais também influenciam a possibilidade de ações não-éticas. As pessoas podem ser tentadas a ter tais atitudes simplesmente porque a entidade dá grandes incentivos para assim agirem. Por exemplo, grandes pressões para obtenção de resultados em curto prazo podem gerar um ambiente interno de desrespeito a padrões éticos de comportamento e a leis e regulamentos. Recompensas salariais altamente dependentes de desempenho financeiro podem gerar práticas questionáveis ou fraudulentas de divulgação de resultados.

A remoção ou redução desse tipo de incentivos contribui para a eliminação de comportamentos não-éticos. Por exemplo, definir alvos de desempenho realistas, seguido de controles apropriados para o sistema de divulgação de resultados.

A ignorância é, também, fator de práticas inapropriadas. Os valores éticos não só devem ser comunicados mediante o exemplo. Devem ser objeto de codificação formal, tais como códigos de ética ou de conduta, que se constituem a base de programas de ética efetivos. Tais códigos definem uma série de questões comportamentais, como integridade e ética, conflitos de interesse, pagamentos ilegais ou de alguma forma impróprios e acordos que frustrem a competição.

De particular importância é a existência de mecanismos de repreensão a condutas de violação das regras, de mecanismos que incentivem as pessoas a denunciar

tais violações e de ações disciplinares contra funcionários que não comunicarem as violações que têm conhecimento. Assim, são necessários canais de comunicação nos quais os funcionários se sintam confortáveis a trazer questões relevantes ao conhecimento de seus superiores.

A existência, porém, de códigos de conduta e sua divulgação apropriada não garante que eles estejam sendo seguidos. É necessário o exemplo vindo de cima, que as ações da gerência sigam o escrito. O conhecimento de que o presidente da entidade agiu eticamente quando confrontado com uma situação difícil é uma mensagem poderosa encaminhada a toda a organização.

Compromisso com Competência

A competência reflete o conhecimento e habilidades necessárias para a realização de tarefas, devendo ser objeto de definição por parte da gerência. Um fator a ser considerado é a natureza e o grau de julgamento que cada tarefa específica deve ter, aliado a um possível compromisso entre supervisão e grau de julgamento individual.

Filosofia e Estilo Operacional da Gerência

São fatores que afetam a forma como a empresa é gerenciada, incluindo o nível de risco que é aceito. Estão relacionados à preferência pelo uso de princípios contábeis agressivos ou conservadores e ao grau de conservadorismo empregado quando do uso de estimativas. Também relacionados ao tipo de atitude tomada quanto à divulgação de demonstrativos financeiros, quanto ao uso de tecnologia de informação, e quanto a processos de negócios e política de pessoal.

Estrutura Organizacional

O modo como uma organização está estruturada reflete a forma como ela planeja, executa, controla e monitora suas atividades. Para possuir uma estrutura adequada, uma organização deve definir áreas chaves de autoridade e responsabilidade, e estabelecer linhas de comunicação apropriadas. Por exemplo, a área de auditoria interna deve ser montada de modo a gerar rapidez de ação, tendo garantido acesso irrestrito à mais alta gerência da empresa, permitindo o cumprimento de suas responsabilidades.

A estrutura da empresa é função de seu tamanho e de sua natureza, mas deve existir de tal forma a permitir um trabalho efetivo de gerenciamento de risco, e a execução de atividades que levem ao alcance dos objetivos.

Designação de Autoridade e Responsabilidade

Envolve o grau no qual indivíduos e equipes são autorizados e encorajados a usar iniciativa para debater assuntos e resolver problemas, assim como limites de autoridade. Também inclui o estabelecimento de canais de comunicação e protocolos de autorização. E diz respeito a políticas que descrevam práticas apropriadas de negócios, conhecimento e experiência de pessoal chave, e fontes existentes para a solução de questões.

Dois desafios são: saber delegar autoridade e responsabilidade na extensão necessária à consecução dos objetivos empresariais; e garantir que todas as pessoas entendam a importância de suas funções para o alcance desses objetivos.

É importante reconhecer que a mudança da estrutura empresarial, com aumento da delegação de competências e correspondente aumento de responsabilidades, deve vir acompanhada de um incremento nas habilidades dos empregados, assim como de sua noção da obrigatoriedade de prestar contas pelos seus atos.

Tais práticas requerem procedimentos adequados de controle por parte da gerência, os quais monitorem os resultados, a fim de que decisões possam ser aceitas ou modificadas a tempo, se necessário.

Políticas e Praticas de Recursos Humanos

Relacionam-se à forma pela qual a empresa realiza atividades de contratação, orientação, treinamento, avaliação, aconselhamento, promoção e punição de pessoal, além de como os empregados são comunicados acerca dos níveis desejados de integridade, comportamento ético e competência.

Envolve a forma como a entidade encara o processo de educação e treinamento de seus empregados, para agir em mercados em constante mutação. Tal processo deve ser contínuo.

Diferenças no Ambiente e Suas Implicações

Diz respeito à identificação de diferentes ambientes passíveis de existir dentro de uma organização, ou entre uma organização e suas subsidiárias. Tais diferenças devem ser conhecidas e tratadas, para que se obtenha sucesso no gerenciamento de risco da entidade como um todo.

É citado o exemplo, ainda que não nominal, provavelmente da empresa Enron, gigante norte-americana do setor de energia, que faliu após escândalos envolvendo

fraudes em demonstrativos financeiros para gerar uma lucratividade fictícia, que beneficiava diretores com o pagamento a mais de bônus:

> Pensava-se que uma conhecida empresa de energia possuía um processo de gerenciamento de risco efetivo, uma vez que existiam gerentes seniores respeitados e de alta capacidade, um conselho de diretores de prestígio, uma estratégia inovadora, sistemas de informação e de controle bem desenhados, manuais de políticas abrangentes descrevendo riscos e funções de controle, e rotinas de supervisão e reconciliação abrangentes. Seu ambiente interno, no entanto, era significativamente falho.
> Os gerentes participavam de práticas comerciais altamente questionáveis, e o conselho de diretores fechava os olhos a essas práticas. Descobriu-se que a companhia apresentava resultados financeiros deturpados, e, com isso, sofreu uma perda de confiança dos acionistas, uma crise de liquidez e a destruição do valor da entidade. Por fim, a companhia sofreu uma das maiores falências da história (COSO, 2003b, p.27, tradução nossa).

3.2 **Definição de Objetivos**

A definição de objetivos é uma pré-condição para a identificação de eventos, para a avaliação de riscos e para a resposta ao risco. Primeiro devem existir objetivos antes que a gerência possa identificar riscos à sua consecução e tomar as ações necessárias para mitigar tais riscos.

Objetivos Estratégicos

É importante que a direção de uma entidade, em conjunto com seu conselho diretor, defina explicitamente a sua missão, isto é, a sua razão maior de existência. A partir daí, são definidos objetivos estratégicos, formuladas estratégias e estabelecidos objetivos relacionados para a organização. Enquanto a missão e os objetivos estratégicos de uma entidade são geralmente estáveis, sua estratégia e objetivos relacionados são mais dinâmicos, ajustando-se a mudanças das condições internas e externas.

Os objetivos estratégicos são metas de alto-nível, alinhados e dando suporte à missão da entidade. Refletem as escolhas dos gerentes sobre como a entidade irá gerar valor às partes interessadas.

Ao considerar diferentes estratégias para alcançar seus objetivos estratégicos, a gerência identifica os riscos associados e suas implicações. Nesse momento, o gerenciamento de risco verifica se as estratégias escolhidas estão compatíveis com o nível de risco que a entidade aceita correr, isto é, com seu apetite ao risco.

Objetivos Relacionados

Após definir objetivos estratégicos e as estratégias para alcançá-los, a entidade é levada a definir objetivos relacionados a níveis operacionais, com o alcance dos quais se criará e preservará valor. São objetivos com foco mais direto nas atividades da organização, tais como vendas, produção, engenharia e funções de infra-estrutura.

Ao se definir objetivos mais específicos de cada área da entidade, é possível o estabelecimento de fatores críticos de sucesso, que são elementos chaves que devem acontecer para que as metas sejam atingidas. Tais elementos devem ser construídos de tal forma que permitam sua medição para acompanhamento e checagem. Além disso, o gerenciamento de risco requer que todas as pessoas tenham conhecimento dos objetivos da empresa naquilo que se referir a sua esfera de atuação.

Categorias de Objetivos Relacionados

Três grandes categorias de objetivos relacionados podem ser identificadas:

- Objetivos Operacionais: relacionam-se à efetividade e eficiência das operações da empresa, incluindo metas de desempenho e lucratividade e guarda de recursos contra perdas. Variam de acordo com as escolhas da gerência sobre estrutura e desempenho, as quais refletem o negócio, a indústria e a economia a que está sujeita a organização. A definição clara de um conjunto de objetivos operacionais é fundamental para o sucesso da empresa, pois, entre outras razões, são eles que direcionam a alocação dos recursos existentes.
- Objetivos de Divulgação: referem-se à confiança das divulgações da empresa. Incluem divulgações internas e externas e podem envolver informação financeira e não-financeira. Seu alcance proporciona aos gerentes informações completas e apropriadas para o processo de tomada de decisão e para o monitoramento das atividades e desempenho da empresa. Proporciona, também, confiança aos clientes externos no que se refere aos seus informes, tais como: demonstrações contábeis, relatórios de gestão e documentações para agentes reguladores.
- Objetivos de Conformidade: relacionam-se à aderência a leis e regulamentos relevantes. Dependem de fatores externos como regulação, e tendem a ser os mesmos para todas as entidades, em alguns casos, ou somente para aquelas pertencentes a um ramo de negócio, em outros casos. Estabelecem padrões mínimos de comportamento e podem, dependendo do seu alcance ou não, comprometer significativamente a reputação da entidade perante a comunidade e o mercado.

Os objetivos de conformidade e de divulgação externa são impostos por leis e regulamentações, havendo pouca oportunidade de mudança por parte das entidades. No entanto, os objetivos operacionais e os de divulgação interna são baseados mais em preferências, julgamentos e estilo de gerência, variando largamente entre as organizações.

As classificações dos objetivos nessas três categorias não são absolutas. Dependendo das circunstâncias, um objetivo pode se encaixar em mais de uma classificação.

Alcance de Objetivos

Tendo sido estabelecidos os objetivos empresariais e classificados conforme as três categorias apresentadas, é importante se notar que há diferenças no nível de segurança existente quanto à certeza de alcance desses objetivos.

Quando se trata de objetivos de divulgação e de conformidade, a atividade de gerenciamento de risco pode prover segurança razoável de que estejam sendo obtidos. O alcance desses objetivos está dentro do controle da entidade, isto é, depende dela fazer o que é necessário para atingi-los.

No entanto, a consecução dos objetivos operacionais depende, por vezes, de fatores externos à entidade, que estão fora do seu controle, tais como mudanças em governos e problemas climáticos. Tais tipos de fatores externos podem ter sido considerados quando da formulação dos objetivos e tratados como de baixa probabilidade, com planos de contingência em caso de ocorrência. Mas, ainda assim, esses planos apenas mitigam seus impactos. Eles não garantem a consecução dos objetivos operacionais.

Dessa forma, as operações de gerenciamento de risco focam primariamente em: desenvolver a consistência dos objetivos e metas operacionais através da organização; identificar fatores de sucesso e riscos; avaliar os riscos e implementar respostas adequadas; estabelecer os controles necessários; e, oportunamente, informar o desempenho e possibilidades. Com isso, o gerenciamento de risco pode fornecer segurança relativa de que a gerência e o conselho de diretores serão informados, a tempo, de como a entidade está se movendo na direção do alcance dos objetivos operacionais.

Seleção de Objetivos

O gerenciamento de risco efetivo não determina quais objetivos serão escolhidos, pois se trata de tarefa dos gerentes da entidade. Mas garante que as gerências, em todos os níveis, possuem um processo que alinha os objetivos à missão e estratégias da entidade, e que os objetivos escolhidos são consistentes com o apetite ao risco.

Tolerância ao Risco

Tolerância ao risco é uma medida do nível aceitável de variação relativa ao alcance dos objetivos. Utiliza as mesmas unidades de medida dos objetivos, estando relacionada ao grau de importância de cada objetivo específico, de forma que a tolerância tende a ser menor quanto ao nível de alcance de objetivos mais críticos.

A operação dentro de padrões de tolerância provê maior segurança de que a entidade se encontra dentro do apetite ao risco desejado, aumentando a confiança no alcance dos objetivos definidos.

3.3 **Identificação de Eventos**

Eventos

Um evento é um incidente ou uma ocorrência emanada de fontes internas ou externas que pode afetar a implementação da estratégia ou o alcance dos objetivos. Pode ter impacto positivo, negativo, ou ambos.

No estágio inicial de identificação de eventos, deve-se tentar considerar todos os eventos com potencialidade de ocorrência, tendo a visão da entidade como um todo. Nessa fase não se deve importar com os possíveis efeitos ou com a probabilidade de ocorrência, que fazem parte da fase de avaliação dos riscos. Com isso evita-se negligenciar eventos relevantes.

Existem limitações práticas que freqüentemente dificultam saber até que ponto se avançar na identificação dos eventos. No entanto, mesmo eventos com baixa probabilidade de ocorrência devem ser considerados, se os efeitos para o alcance dos objetivos forem elevados.

Fatores que influenciam Estratégias e Objetivos

Identificar fatores que influenciam a implementação de estratégias e o alcance de objetivos é útil para a identificação de eventos efetiva. Devem ser considerados fatores presentes, assim como os que podem ocorrer no futuro. A tabela a seguir apresenta uma possível relação de fatores internos e externos à entidade.

Tabela 2 – Categorização de Eventos

Categorias de Eventos		
Fatores Internos	**Fatores Externos**	
Infra-estrutura • disponibilidade dos bens • capacidade dos bens • acesso a capital • complexidade • fusões/aquisições **Pessoal** • capacidade dos empregados • atividade fraudulenta • saúde e segurança • delitos • práticas de segurança • práticas de vendas **Processo** • capacidade • projeto	**Econômicos** • disponibilidade de capital • crédito o emissão o falta de pagamento o concentração • liquidez o negociações o financiamento o fluxo de caixa • mercado o preços de *commodities* o taxa de juros o desemprego o índices	**Tecnológicos** • comércio eletrônico • dados externos • tecnologias emergentes **Meio-Ambiente** • biodiversidade • emissões, efluentes e desperdício • energia • fogo • desastres naturais • desenvolvimento sustentável • transporte

Categorias de Eventos		
Fatores Internos	**Fatores Externos**	
• execução • fornecedores/dependências **Tecnologia** • dados o aquisição o manutenção o distribuição o confidencialidade o integridade • diponibilidade de dados e sistemas • capacidade • sistemas o seleção o desenvolvimento o posicionamento estratégico o confiança	o taxa de câmbio o avaliação justa o valores de mercado **Negócios** • marcas e patentes • competição • comportamento do consumidor • contrapartida • fraude • padrões industriais • estrutura proprietária • publicidade • relevância do produto	• água **Políticos** • mudanças governamentais • legislação • políticas públicas • regulação **Sociais** • questões demográficas; • cidadania • liderança ambiental • privacidade

Fonte: COSO, 2003b, p.44, tradução nossa.

Além de identificar eventos que afetem a entidade em si, deve-se tentar identificar eventos que afetam níveis de atividades, tais como vendas, produção, *marketing*, desenvolvimento tecnológico e pesquisa e desenvolvimento. Com isso, melhora o nível de avaliação de riscos em grandes áreas de negócio.

Metodologias e Técnicas de Identificação de Eventos

As técnicas de identificação de eventos podem olhar tanto para o passado como para o futuro. Variam grandemente no nível de sofisticação, e na forma como são empregadas nas diferentes entidades. A escolha da metodologia deve se basear na cultura de risco da organização, e ser robusta o suficiente, uma vez que é a base para os componentes de avaliação de risco e resposta ao risco do modelo.

As sete técnicas a seguir são apresentadas como exemplo pelo documento COSO:

- inventário de eventos: são listas detalhadas de eventos potenciais comuns a companhias dentro de uma indústria particular, ou de um processo ou atividade comum entre as indústrias. *Softwares* comerciais podem gerar listas relevantes e seus riscos associados. Algumas entidades usam essas listas como ponto de partida para a atividade de identificação de eventos;
- análise interna: pode ser feita como parte de um ciclo de planejamento de negócio rotineiro, tipicamente via reuniões de equipes. Algumas vezes

são utilizadas informações de outros interessados (consumidores, fornecedores ou outras unidades de negócio), ou submetidas informações a especialistas de fora da unidade (especialistas internos ou externos da área de negócio, ou equipe de auditoria interna);

- indicadores de limiar ou escalas: os indicadores alertam os gerentes de áreas em questão ao comparar transações correntes, ou eventos, com critérios pré-definidos. Uma vez medido, um evento pode requerer avaliação posterior ou respostas imediatas. Por exemplo, pode-se monitorar volumes de vendas em mercados baseado em novos programas de *marketing* ou propaganda e redirecionar os recursos baseado nos resultados. Ou pode-se acompanhar a estrutura de preços de competidores e avaliar a mudança de sua própria estrutura de preços quando certos limiares forem atingidos;
- entrevistas e grupos de discussão facilitados: essa técnica identifica eventos em discussões estruturadas, a partir do conhecimento e experiência acumulada de gerentes, equipe ou outros interessados. O facilitador ou entrevistador comanda a discussão sobre eventos que podem impactar o alcance dos objetivos da unidade ou toda entidade;
- indicadores de eventos condutores: ao monitorar dados relativos a eventos, as entidades identificam a existência de condições que podem gerar outros eventos. Por exemplo, instituições financeiras identificam a correlação entre o atraso no pagamento de empréstimos e o possível não pagamento da dívida, gerando a ação de intervenção prévia;
- dados de eventos de perdas: a existência de dados relativos a eventos de perdas é uma fonte útil na identificação de tendências e causas. Uma vez que uma causa foi identificada, pode-se considerar mais efetivo a sua avaliação e tratamento do que a consideração de um novo evento;
- análise do fluxo do processo (mapa de processos): considera a combinação de entrada, tarefas, responsabilidades e saídas que se combinam para formar um processo de trabalho. Ao considerar os fatores internos e externos que afetam as entradas ou tarefas de um processo, identificam-se os eventos que podem afetar o alcance dos objetivos do processo.

Interdependência de eventos

Os eventos não ocorrem sozinhos. Assim, na sua identificação, deve-se entender como eles se inter-relacionam, de forma a melhor direcionar os esforços de gerenciamento de riscos.

Categorias de Eventos

É útil o agrupamento dos eventos identificados em categorias. Ao agregá-los, desenvolve-se conhecimento acerca dos seus inter-relacionamentos, além de se poder verificar se o trabalho até então executado está completo.

A forma de categorização pode variar de entidade para entidade. Exemplos são: a agregação dos eventos horizontalmente através da entidade e verticalmente dentro das unidades operacionais; ou basear-se em uma categorização dos objetivos da entidade, partindo-se dos de mais alto nível, para então cair nos objetivos relevantes para as unidades organizacionais, funções e processos de negócio.

A tabela 2, anteriormente apresentada, mostra uma categorização baseada em fatores internos e externos.

Distinguindo Riscos e Oportunidades

Os eventos podem ter um impacto negativo, positivo ou ambos. Eventos potencialmente negativos representam riscos e devem ter avaliação e resposta. Eventos com possível impacto positivo representam oportunidades ou compensação a impactos negativos de riscos.

Eventos que representam oportunidades devem ser canalizados de volta ao processo de definição de estratégias e objetivos, com o intuito de formular ações para aproveitar essas oportunidades. Eventos que são compensações a riscos são considerados nas etapas de avaliação e resposta aos riscos.

3.4 **Avaliação de Risco**

Contexto para a Avaliação de Risco

Risco é a possibilidade de que um evento ocorra e afete negativamente o alcance de objetivos.

Fatores internos e externos influenciam eventos, e embora alguns desses fatores sejam comuns a qualquer organização, muitos são únicos para cada entidade devido aos seus objetivos estabelecidos e às suas escolhas no passado.

Riscos Intrínsecos e Residuais

Ricos intrínsecos são aqueles existentes na ausência de qualquer ação para alterar sua probabilidade e impacto.

Riscos residuais são aqueles que se mantêm depois de aplicadas ações de resposta ao risco.

Estimando Probabilidade e Impacto

Uma característica dos riscos é a incerteza quanto a sua ocorrência. Para se trabalhar essa incerteza, avalia-se o risco a partir de duas perspectivas: probabilidade, que representa a possibilidade de ocorrência do evento, e impacto, que representa o efeito em caso de ocorrência.

A probabilidade pode ser medida por termos qualitativos, tais como alta, média ou baixa, ou quantitativos, como medidas de porcentagem, freqüência ou outras escalas métricas. As unidades de medida do impacto dos riscos normalmente seguem as mesmas unidades de desempenho utilizadas na medição do alcance dos objetivos.

As estimativas de probabilidade e impacto freqüentemente são feitas utilizando dados observáveis do passado, que provêm uma base mais objetiva do que estimativas inteiramente subjetivas. Deve-se ter cuidado ao se utilizar dados passados para se fazer previsões sobre o futuro, uma vez que os fatores que influenciam os eventos podem variar com o tempo.

É necessário ter atenção com o horizonte temporal dos riscos. Certos objetivos estratégicos se referem a questões de longo prazo, devendo ser considerada a escala de tempo adequada a cada caso.

A forma de apresentação do binômio probabilidade x impacto é variada. Podem ocorrer estimativas de valores esperados ou de pior-caso, distribuições ou escalas, ou descrições por escrito. Uma forma comum é a colocação em gráficos, tais como os

mapas de risco, que explicitam os eventos por categoria, objetivos organizacionais ou outros tipos de agrupamento.

Uma tarefa desafiadora é determinar quais riscos devem ser objeto de atenção. É mais fácil com riscos de pouca probabilidade e baixo impacto, que normalmente não demandam muita atenção e com riscos de alto impacto e probabilidade, que devem ter tratamento diferenciado. No entanto, entre esses dois limites, está um gama de riscos de difícil julgamento, que carecem de análise racional e cuidadosa.

Metodologias e Técnicas Qualitativas e Quantitativas

A metodologia de avaliação de risco abrange uma mistura de técnicas qualitativas e quantitativas. Normalmente as técnicas qualitativas são utilizadas em situações nas quais os riscos não podem ser quantificados ou a obtenção de dados quantitativos é de difícil obtenção ou de custo impeditivo.

Técnicas quantitativas tipicamente trazem mais precisão e são utilizadas em atividades mais complexas e sofisticadas, algumas vezes com a utilização de modelos matemáticos. Essas técnicas são dependentes da qualidade dos dados de suporte e de suposições, e são mais adequadas a situações com história e freqüência de ocorrência conhecidas, e que permitam previsões confiáveis. Alguns exemplos de técnicas quantitativas são:

- *benchmarking*: um processo de colaboração entre entidades, o *benchmarking*, focando em eventos ou processos específicos, compara medidas e resultados utilizando padrões comuns, e identifica oportunidades de melhoria. Os dados de eventos, processos e medidas são desenvolvidos de forma a comparar os desempenhos. É utilizado por algumas companhias para avaliar o impacto e a probabilidade de eventos dentro de uma indústria;
- modelos probabilísticos: associam uma escala de eventos e o impacto resultante com a probabilidade de ocorrência baseado em certas hipóteses, que envolvem dados históricos ou resultados simulados que refletem suposições de um comportamento futuro. Podem ser usados em diferentes horizontes de tempo para estimar resultados como a escala de valores de um instrumento financeiro no tempo, ou para estimar o resultado de um evento sob condições extremas ou inesperadas;
- modelos não-probabilísticos: usam hipóteses subjetivas para estimar o impacto de eventos sem quantificar uma probabilidade associada. A

> avaliação de eventos é baseada em dados históricos ou simulados e em previsões de comportamentos futuros. Exemplos são: medidas de sensibilidade, teste de stress e análise de cenários.

Para ganhar consenso quanto às avaliações qualitativas podem ser usadas as mesmas técnicas de identificação de eventos, tais como entrevistas e grupos de discussão.

A existência de abordagens qualitativas e quantitativas leva a uma expressão qualitativa do binômio impacto x probabilidade. Para se considerar uma abordagem como quantitativa é necessária a integralidade das abordagens nessa técnica.

Correlação de eventos

Deve-se avaliar como os eventos existentes podem se correlacionar de forma a modificar o impacto e probabilidade de eventos isolados. Podem ser usados testes de stress para avaliar o impacto de eventos extremos e análise de cenários para avaliar os efeitos de múltiplos eventos. Verificar a correlação de probabilidades e impactos de eventos é uma importante responsabilidade do gerenciamento de risco.

3.5 **Resposta ao Risco**

Identificação da Resposta ao Risco

A ação de analisar os riscos intrínsecos e avaliar respostas visa a atingir um risco residual que se enquadre na tolerância ao risco da entidade. São quatro as possibilidades de resposta ao risco: fuga; redução; compartilhamento; e aceitação.

Na fuga a ação é no sentido de evitar as atividades que geram risco. Os motivos podem ser um custo de resposta superior ao benefício esperado, ou a ausência de uma resposta capaz de levar o binômio probabilidade x impacto a um valor aceitável. Exemplos: abandonar uma linha de produtos; desistir de expandir para uma nova área geográfica; ou vender parte da empresa.

Na redução a resposta é no sentido de reduzir o binômio probabilidade x impacto, de forma a gerar um risco residual aceitável. Está relacionada a uma infinidade de possíveis ações gerenciais.

No compartilhamento transfere-se parte do risco a outrem de forma a, também, trazer o risco residual para dentro da tolerância aceitável. Técnicas comuns de compartilhamento incluem seguros, distribuição de risco, operações de *hedging* e terceirização de atividades.

Na aceitação não se toma nenhuma ação quanto ao risco, indicando que o risco intrínseco já está dentro do nível de tolerância.

Avaliação de Possíveis Respostas aos Riscos

Na escolha das possíveis respostas aos riscos, deve-se considerar alguns aspectos. Primeiro, não se deve perder de vista que, por vezes, a combinação de respostas possíveis pode trazer resultados mais eficazes, o que reforça a importância de categorizar os eventos e riscos de forma a possuir uma visão integrada.

Ações de resposta podem agir diferentemente sobre o impacto e sobre a probabilidade dos eventos. Por exemplo, uma possível ação para mitigar os efeitos de um terremoto sobre um centro de computação é um plano de contingência. No caso, a ação é somente sobre o impacto do evento, já que nada está sendo feito quanto à probabilidade de ocorrência. Outra opção seria deslocar o centro para uma região de maior estabilidade sísmica, o que diminui a probabilidade de ocorrência do evento, mas não o seu impacto.

É fundamental a análise do custo x benefício das respostas. No entanto, tal análise nem sempre é de fácil realização. Geralmente, a consideração do custo é mais

imediata, mas, ainda assim, pode apresentar dificuldades, a exemplo da quantificação de tempo e esforço. Também difícil é lidar com certos fatores como o comprometimento da gerência com valores éticos ou a percepção da preferência de consumidores.

A análise dos benefícios pode ser ainda mais sujeita a considerações subjetivas. No entanto, certos fatores internos podem ser usados para avaliar possíveis benefícios: a probabilidade de ocorrência de um evento não desejado; e a natureza do evento e seus potenciais efeitos financeiros e operacionais para a entidade. Isto é, a análise dos benefícios é feita pela consideração da não ocorrência do evento negativo.

Da mesma forma que a identificação de eventos pode trazer a percepção de oportunidades, que deverão ser canalizadas para a definição das estratégias e objetivos, por vezes, as respostas aos riscos acabam por se traduzir, também, em oportunidades. Isso pode acontecer quando as possíveis respostas estão no limite de sua efetividade e refinamentos posteriores somente trazem ganhos marginais na probabilidade e impacto. Por exemplo, a resposta criativa de uma companhia de seguros de automóveis ao alto número de acidentes de um entroncamento de rodovias. Ela decidiu financiar melhoramentos na sinalização de trânsito, reduzindo as reclamações por acidente e aumentando suas margens de lucro.

Importante se ter consciência de que as respostas aos riscos são, por si só, eventos. Portanto, estão sujeitas, também, a riscos, que devem ser analisados.

Entidades sujeitas a diferentes riscos em cada uma de suas unidades devem receber um tratamento que considere uma visão integrada dos riscos. Dessa forma, deve-se verificar se os riscos residuais em cada unidade estão dentro do nível de tolerância, e se a integração dos riscos mantém o risco da entidade dentro desse nível. Podem ser necessárias novas ações no sentido de adequar a situação do todo.

Respostas Selecionadas

A ação de decidir quais respostas aos riscos serão utilizadas não é do gerenciamento do risco. Trata-se de uma atividade tipicamente gerencial. Da mesma forma, a implementação dessas respostas, de forma a recalibrar o risco a níveis residuais, é função de cada gerente. Cabe, ainda a cada gerente desenvolver procedimentos que assegurem a implementação efetiva. Esses procedimentos representam atividades de controle.

Deve-se reconhecer que certos riscos residuais sempre existirão, não só devido à escassez de recursos, mas também às incertezas futuras e às limitações de quaisquer atividades.

3.6 **Atividades de Controle**

Atividades de controle são políticas e procedimentos, os quais constituem as ações das pessoas para implementar as políticas, que devem ajudar a assegurar que as respostas aos riscos estão sendo executadas de maneira apropriada e em tempo correto. Constituem parte do processo pelo qual uma entidade busca atingir seus objetivos empresariais, sendo aplicadas em relação a cada uma das quatro categorias de objetivos: estratégicos; operacionais; de divulgação; e de conformidade.

Para ilustrar a relação entre objetivos, resposta aos riscos, e controles verifique-se a situação de uma empresa que deseja alcançar ou suplantar suas metas de vendas. Entre os riscos está o de não ter conhecimento suficiente de fatores externos como necessidades atuais e potenciais dos consumidores. Para reduzir a probabilidade de ocorrência e o impacto do risco, a gerência decidiu obter informações sobre os hábitos de consumo existentes e tomar para si a inicitiva de criar novas necessidades. Essas respostas ao risco servem como ponto focal no estabelecimento das ações de controle, que podem incluir seguir o progresso no tempo da atividade de obtenção de informações sobre os hábitos de consumo, e tomar medidas que assegurem a precisão desses dados. Dessa forma, as atividades de controle são construídas diretamente dentro do processo de gerenciamento, o que minimiza a noção de que elas devam existir meramente por obrigação.

São variados os tipos de atividade de controle, entre os quais se pode citar os controles preventivo ou detectivo e manual ou automatizado. Algumas atividades típicas são:

- supervisão funcional ou gerenciamento de atividades: gerentes de atividades ou funções revêem relatórios de desempenho;
- processamento de informação: uma variedade de controles são executados para garantir a exatidão, integridade e autorização de transações;
- controles físicos: realização de inventários periódicos, nos quais os bens são contados e o montante comparado com valores existentes em relatórios de controle;
- indicadores de desempenho: relacionamento entre si de diferentes dados – operacionais ou financeiros – junto com análises das relações e possíveis ações corretivas.

Políticas e Procedimentos

As atividades de controle normalmente envolvem dois elementos. As políticas, que estabelecem o que deve ser feito, e os procedimentos, que estabelecem como deve ser feito.

Há situações em que as políticas são estabelecidas oralmente. Tais situações podem ser efetivas se referirem a práticas já absorvidas e bem entendidas, ou em pequenas empresas, nas quais os canais de comunicação envolvem apenas pequenas camadas e há uma forte interação entre supervisão e execução.

O que é mais importante, no entanto, é que as políticas devem ser realizadas de uma maneira ponderada, consciente e consistente. Um procedimento não será útil se executado mecanicamente e sem foco contínuo nas diretrizes da política. Dessa forma, é essencial que se investigue as condições resultantes das ações de controle, e que se tome as medidas corretivas, quando necessárias. Esse acompanhamento varia dependendo do tamanho e da estrutura organizacional da entidade. Há estruturas formais de informação em grandes companhias, nas quais unidades de negócio declaram porque metas não foram atingidas e as ações que estão sendo tomadas para evitar repetições. E há situações de pequenas empresas nas quais o proprietário caminha pelos corredores questionando sobre o que aconteceu de errado e o que precisa ser feito.

Controles sobre Sistemas de Informação

Há dois grandes agrupamentos de controles sobre sistemas de informação: controles gerais e controles de aplicativos.

Os controles gerais servem à maioria, senão a todos os sistemas e ajudam a garantir a continuidade e operação apropriada. Alguns controles comuns desse tipo são:

- gerenciamento da tecnologia da informação: um comitê de direção provê supervisão, monitoramento e divulgação sobre as atividades de tecnologia da informação, além de iniciativas de melhoria;
- infra-estrutura da tecnologia de informação: controles são aplicados às áreas de definição, aquisição, instalação, configuração, integração e manutenção de sistemas. Os controles podem incluir acordos de prestação de serviços que estabeleçam e aumentem o desempenho de sistemas, planos de contingenciamento que mantenham os sistemas disponíveis, checagem do desempenho operacional para verificação de falhas e programação da operação dos computadores. Os *softwares*

podem incluir controles como revisão e aprovação pela gerência ou pelo comitê de direção de novas aquisições significativas, restrição de acesso e configuração a *softwares* de sistema operacional, reconciliações automáticas de dados, e detecções para erros de comunicação. Podem incluir, também, rastreamento de incidentes e controle de acesso e de alteração de dados em utilitários;

- gerenciamento de segurança: protege contra acesso inapropriado e uso não autorizado. É controlado o acesso, via senha de segurança, à rede, ao banco de dados e aos aplicativos. Contas de usuário permitem o acesso somente às funções necessárias ao desempenho de tarefas específicas. *Softwares* de *firewall* para internet e redes privadas virtuais protegem os dados de acesso externo não autorizado;
- aquisição, desenvolvimento e manutenção de *software*: processos definidos que incluem requisitos de documentação, testes de aceitação de uso, testes de stress e avaliação de risco de projeto. O acesso a códigos fonte é controlado por bibliotecas de códigos. Desenvolvedores de *software* trabalham somente em ambientes separados de desenvolvimento e teste, e não têm acesso ao ambiente de produção. Controles sobre mudanças de sistemas incluem autorização para efetivação, revisão das mudanças, aprovações, documentação, teste, impacto das mudanças em outros componentes do sistema de tecnologia de informação, resultados de testes de stress e protocolos de implementação.

Os controles de aplicativo são designados a garantir integridade, exatidão, autorização e validade de dados capturados e em processamento. Aplicativos individuais podem depender de controles de operação efetivos sobre sistemas de informação para assegurar que os dados são capturados ou gerados quando necessários, que os aplicativos de suporte estão disponíveis e que erros de *interface* são detectados rapidamente.

Uma das mais significativas contribuições dos computadores é a capacidade de prevenir a entrada de erros no sistema, assim como detectá-los e corrigi-los quando presentes. Para tanto, controles de aplicativo dependem de checagens de edição computadorizadas. Trata-se de verificações de formato, existência e razoabilidade dos dados, entre outras, que são embutidas nos aplicativos durante o desenvolvimento.

Quando projetadas adequadamente, essas verificações podem prover controle sobre dados de entrada.

Alguns exemplos de controles de aplicativo são:

- atividades de balanceamento de controle: detectam erros em dados via reconciliação com um controle total de montantes capturados manualmente ou automaticamente;
- verificações digitais: cálculos para validar dados;
- listas de dados pré-definidas;
- testes de razoabilidade de dados: comparam os dados capturados com padrões de razoabilidade;
- testes lógicos: incluem o uso de limites de variação, ou testes de valor ou alfanuméricos.

Especificidades de Entidades

Cada entidade é única na sua complexidade, história, cultura, pessoal, entre outras características que afetam as atividades de controle. Mesmo que duas organizações tenham objetivos idênticos e apresentem decisões semelhantes sobre como atingi-los, suas atividades de controle tendem a ser diferentes.

3.7 **Informação e Comunicação**

Informação

Qualquer organização tem acesso a informações, financeiras ou não, relacionadas a atividades internas ou externas, que são relevantes para o seu gerenciamento. Essas informações devem estar disponíveis aos interessados de uma maneira e a tempo tais que permitam o adequado gerenciamento de risco, assim como o cumprimento de outras obrigações.

As informações são utilizadas no alcance dos quatro tipos de objetivos das organizações: estratégicos, operacionais, de divulgação e de conformidade. Ocorre uma grande inter-relação entre essas variáveis, de forma que a mesma informação financeira ou operacional, por exemplo, pode ser utilizada no alcance dos quatro objetivos.

Os dados estão disponíveis, muitas vezes, a partir de fontes internas e externas variadas e em múltiplas formas. O grande desafio do gerenciamento é saber filtrar e processar esses dados de forma a transformá-los em informações relevantes. Para tanto é necessário o desenvolvimento de uma estrutura de pesquisa, captura, processamento, análise e divulgação de dados internos e externos.

Esses sistemas de informação podem ser formais ou informais. Informações críticas para identificar riscos e oportunidades podem vir de conversas com consumidores, fornecedores, reguladores e os próprios funcionários, assim como da participação em seminários e feiras e associações profissionais.

Manter sistema de informações consistente com suas necessidades é ainda mais importante para organizações que enfrentam mudanças fundamentais na indústria, competição inovadora ou trocas significativas nas demandas dos consumidores.

Sistemas Estratégicos e Integrados

O projeto da arquitetura de sistemas de informação e a aquisição de tecnologia são aspectos relevantes da estratégia de uma entidade. As escolhas envolvendo a tecnologia podem ser críticas quanto à obtenção dos objetivos, e essa realidade é ainda mais marcante à medida que os negócios necessitam de mudanças e as tecnologias criam novas oportunidades de vantagem estratégica. Tais escolhas dependem de variados fatores, incluindo as metas organizacionais, as necessidades de mercado e as características do processo competitivo. Enquanto os sistemas de informação são fundamentais para o gerenciamento de risco, as técnicas deste podem ajudar nas escolhas acerca das tecnologias.

É comum a integração total dos sistemas de informação à maioria dos aspectos operacionais. Operações e sistemas baseados em rede (internet e intranet), e sistemas de ERP[19] (*enterprise resource planning*) são cada vez mais utilizados. Essas aplicações facilitam o acesso geral a informações que, normalmente, estariam disponíveis somente para os departamentos e funções específicas que as geram.

Para um efetivo gerenciamento de risco são utilizados dados históricos e atuais. Dados históricos permitem que seja feito batimento do desempenho corrente contra alvos, planos e expectativas. Provêem conhecimento sobre como a entidade costuma responder em diferentes condições, permitindo à gerência identificar correlações e tendências. Servem, também, como alerta de eventos potenciais que devem chamar a atenção.

Dados presentes permitem que seja estabelecido o perfil de risco atual (visão dos riscos existentes em um processo, função ou unidade naquele momento) e verificar se ele se encontra dentro da tolerância desejada. Em conjunto com os dados históricos permitem que sejam desenhados cenários e que se façam projeções de desempenhos futuros. Com isso, torna-se possível a mudança de ações de forma a calibrar o perfil de risco ao apetite ao risco.

A informação necessária para o gerenciamento de risco da entidade é disponibilizada como parte do gerenciamento contínuo, isto é, está integrada com as informações existentes para gerir a entidade. Por exemplo, as informações financeiras não são utilizadas somente para desenvolver os demonstrativos externos obrigatórios, mas também, para gerar relatórios internos e monitorar desempenho.

O grau de profundidade e a oportunidade da disponibilização das informações a cada interessado dentro das organizações são funções dos diferentes níveis de gerenciamento a que cada um está exposto. É certo que os avanços na tecnologia de captura e armazenamento, assim como o barateamento dos custos, têm levado a uma "sobrecarga de informação". Assim, o desafio é assegurar o fluxo da informação correta, na forma correta, no nível preciso de detalhe, para a pessoa certa, no prazo necessário.

O aumento da complexidade e a integração dos sistemas de informação são constantes, surgindo novos riscos, como violações na segurança das informações e

[19] ERP são sistemas que integram todos os departamentos e funções de uma empresa em um único sistema computacional, que, operando em tempo-real e com base de dados única, deve servir às necessidades específicas de cada área.

crimes cibernéticos. Esses novos riscos devem ser integrados ao processo de gerenciamento de riscos das entidades.

Qualidade da Informação

Com a maior dependência dos sistemas de informação, ter confiança nos dados disponibilizados é característica crítica. Dados inexatos ou errados podem resultar em riscos não previstos ou avaliações pobres e decisões gerenciais ruins.

Informações com qualidade devem preencher os seguintes requisitos: conteúdo apropriado (nível certo de detalhamento); oportunidade (presente quando necessária); atualidade (ser a última informação disponível); precisão (dados corretos); e acessibilidade (de fácil obtenção para quem precisa). Para obter esse padrão, as entidades estabelecem programas de gerenciamento total de dados, que compreendem a aquisição, a manutenção e a distribuição dos dados e o gerenciamento da informação. Tais programas prevêem, além das responsabilidades relativas à integridade dos dados, a avaliação sistemática de qualidade.

Dada a expansão de atividades como o comércio eletrônico, as informações necessárias ao gerenciamento não são obtidas somente dentro da entidade. Há uma grande troca de dados operacionais, financeiros e de conformidade entre fornecedores, vendedores, consumidores, entre outros. A integridade dessas trocas deve ser mantida, o que aumenta a responsabilidade sobre os sistemas de informação.

Comunicação

A comunicação é inerente a todos os sistemas de informação. Além do fornecimento de informações para o alcance de objetivos, como discutido anteriormente, a comunicação deve acontecer em um sentido mais amplo, lidando com assuntos como expectativas de comportamento e responsabilidades de indivíduos e grupos.

Interna

O processo de comunicação interna deve se alinhar e servir de base com a desejada cultura de risco da entidade. Para tanto, deve, de uma maneira clara, efetivamente:

- garantir o conhecimento da importância e relevância de um gerenciamento de risco efetivo;
- informar a filosofia de risco, o apetite ao risco e a tolerância ao risco da entidade;
- implementar e manter uma linguagem comum de risco;

- notificar aos funcionários sobre seu papel e responsabilidades no gerenciamento de risco.

As pessoas têm que saber que, quando algo inesperado acontece, deve se dar atenção não somente ao evento em si, mas também às suas causas. Assim, falhas no sistema podem ser identificadas e tomadas ações de modo a impedir re-ocorrências. Têm que saber como suas atividades se relacionam às dos outros, de forma a ajudar a reconhecer um problema ou determinar suas causas e correções. E devem conhecer o que é considerado comportamento aceitável e não-aceitável.

Outro fator primordial são canais de comunicação abertos e uma vontade nítida de ouvir. Os empregados devem acreditar que seus superiores querem saber acerca dos problemas e que irão efetivamente tratá-los. A maioria dos gerentes reconhece que devem evitar cortar os canais de comunicação. Mas, com as pressões do dia-a-dia de trabalho, eles podem se tornar não receptivos a conhecer novos problemas. E as pessoas percebem rapidamente os sinais, falados ou não, de que um superior não tem tempo ou interesse em lidar com os problemas que eles descobriram. Por fim, o gerente não receptivo é o último a perceber que os canais de comunicação se fecharam.

Os canais de comunicação devem garantir, também, que informações relevantes possam ser distribuídas entre unidades, processos ou áreas de uma entidade. E devem existir linhas alternativas de comunicação, a serem utilizadas no caso de falha das regulares. Em algumas companhias há canais diretos com autoridades de maior nível, como o auditor interno chefe.

É importante que os empregados entendam que não haverá represálias por comunicarem informações relevantes. Deve haver uma mensagem clara que encoraje o reporte de atitudes suspeitas contra o código de ética ou conduta.

Um dos mais críticos canais de comunicação é o entre a gerência superior e o conselho de diretores. A gerência deve manter o conselho informado sobre o desempenho, desenvolvimentos, riscos e o funcionamento do gerenciamento de risco, além de outras informações e eventos relevantes. Quanto melhor a qualidade das informações, melhor o conselho poderá desempenhar suas responsabilidades. Da mesma forma, o conselho deve comunicar à gerência superior as informações que ela precisar e fornecer *feedback* e direção.

Externa

Canais abertos de comunicação com consumidores e fornecedores fornecem importantes informações, tanto estratégicas (necessidades e interesses dos

consumidores), quanto operacionais (projeto e qualidade dos produtos). Informações sobre o apetite e tolerância ao risco das empresas envolvidas são necessárias em transações de comércio eletrônico e cadeias de fornecedores, de forma a verificar se as suas próprias características de risco estão sendo resguardadas.

O entendimento de auditores externos acerca das estratégias, operações e sistemas de controle da entidade fornece informações importantes sobre risco e controle.

Manter canais de comunicação pertinentes e oportunos, de acordo com os requisitos legais e regulamentares, com grupos interessados, reguladores, analistas financeiros e outros membros externos fornece as informações relevantes a suas necessidades, além de permitir que eles tenham acesso às circunstâncias e aos riscos que a entidade enfrenta.

Um compromisso sério de comunicação com partes externas, também, direciona uma forte mensagem interna através da entidade.

Meios de Comunicação

A comunicação pode ter a forma de manuais de políticas, memorandos, e-mails, jornais internos, mensagens via rede e por vídeo. Quando as informações forem transmitidas oralmente, o tom de voz e a linguagem utilizada enfatizam o que está sendo dito. A forma como a informação é apresentada pode afetar significativamente sua interpretação, e como os riscos e as oportunidades associadas são vistos.

Outra ferramenta poderosa de comunicação é a forma como os superiores lidam com seus subordinados. As ações valem mais do que as palavras, mas elas são influenciadas pela história e cultura da entidade, refletindo a maneira como situações de risco ou oportunidade foram tratadas no passado.

3.8 **Monitoramento**

O gerenciamento de risco de uma entidade varia com o tempo. Respostas aos riscos que eram efetivas, podem se tornar irrelevantes; atividades de controle podem ficar menos efetivas, ou não serem mais aplicadas; ou os objetivos da entidade podem mudar. Isso pode ocorrer devido à chegada de novos empregados, a mudanças na estrutura ou direção da entidade, ou à introdução de novos processos. Em face dessas mudanças, é preciso estabelecer se os componentes do gerenciamento de risco continuam efetivos.

O monitoramento pode ocorrer mediante processos contínuos ou por avaliações em separado. O gerenciamento de risco normalmente é projetado para ser avaliado de forma contínua, mas alguns fatores podem levar à necessidade de avaliações em separado. Entre esses estão o grau e a natureza de modificações, tanto externas quanto internas, e os riscos associados; a competência e experiência dos funcionários responsáveis pela implementação das respostas aos riscos e dos controles relacionados; e os resultados dos monitoramentos contínuos.

Monitoramento Contínuo

O monitoramento contínuo é construído dentro das operações normais, corriqueiras de uma entidade, sendo realizado em tempo-real, e reagindo dinamicamente às mudanças de condições. Por isso, é mais eficiente do que avaliações em separado, que identificam ocorrências após o fato. Quando uma entidade tem necessidade de freqüentes avaliações em separado, deve avaliar a melhora do monitoramento contínuo mediante a construção ao invés de adição de atividades.

Alguns exemplos de atividades de monitoramento contínuo são:

- relatórios operacionais são integrados ou reconciliados com relatórios de sistema e usados para gerir operações de uma maneira contínua, sendo identificadas de pronto imperfeições significativas ou exceções a resultados esperados;
- modelos de *value-at-risk* são usados para avaliar os impactos de movimentos potenciais de mercado de uma posição financeira da entidade. Esses modelos funcionam como ferramentas efetivas para determinar se as unidades ou funções de negócios estão dentro das tolerâncias de risco identificadas;

- comunicações de partes externas corroboram informações internas ou indicam problemas. Os consumidores implicitamente corroboram dados de faturamento ao pagar suas faturas. De modo oposto, reclamações de clientes sobre erros em faturas podem indicar deficiência nas transações de vendas;
- reguladores podem comunicar-se com a entidade sobre questões de conformidade que refletem no funcionamento do processo de gerenciamento de risco;
- auditores internos e externos e consultores regularmente provêm recomendações para reforçar o gerenciamento de risco. Auditores podem avaliar com bastante atenção os riscos chaves, as respostas aos riscos e o projeto e efetividade dos controles relativos. Fragilidades potenciais podem ser identificadas e ações alternativas serão recomendadas, acompanhadas de informações úteis no tocante à relação custo x benefício. Auditores internos ou outros funcionários executando atividades de revisão podem ser particularmente efetivos quanto à monitoração das atividades da entidade;
- seminários de treinamento, sessões de planejamento e outras reuniões fornecem importante *feedback* sobre a efetividade do gerenciamento de risco. Além dos problemas particulares que podem indicar questões de risco, a consciência sobre riscos e controles dos participantes normalmente fica exposta;
- Os funcionários são chamados periodicamente a explicitar seu entendimento e cumprimento do código de conduta da entidade. Pessoas das áreas operacional e financeira podem, da mesma forma, ser requisitadas a informar se certos controles de procedimentos, tais como reconciliação, são regularmente executados. Essas declarações podem ser verificadas pela gerência ou pela auditoria interna.

Avaliações em Separado

As avaliações em separado fornecem, de tempo em tempo, uma visão da efetividade do gerenciamento de risco e do próprio monitoramento contínuo.

Escopo e Freqüência

Normalmente as avaliações em separado se concentram em partes específicas do gerenciamento de risco. A decisão de se realizar uma avaliação total pode vir a partir de: mudanças nas estratégias principais ou na gerência superior; grandes aquisições ou vendas; alterações significativas nas condições econômicas ou políticas; ou mudanças significativas nas operações ou nos métodos de processamento de informações.

Quem avalia

Freqüentemente, as avaliações são realizadas na forma de auto-avaliações, nas quais os responsáveis por uma unidade ou função particular determinam a efetividade do gerenciamento de risco para suas atividades.

Os auditores internos normalmente realizam avaliações como parte de suas obrigações regulares, ou a pedido de executivos da empresa ou do conselho de diretores. Da mesma forma, pode ser utilizado o auxílio de auditores externos para se avaliar a efetividade do gerenciamento de risco.

O Processo de Avaliação

A avaliação do gerenciamento de risco é, em si, um processo.

O avaliador deve entender cada uma das atividades da entidade e cada um dos componentes do gerenciamento de risco sob exame. Pode ser útil focar, inicialmente, a maneira como o gerenciamento de risco foi projetado para funcionar. Então, deve-se verificar como o sistema funciona, de fato.

Procedimentos projetados para operar de um modo particular podem ser modificados no correr do tempo, ou não serem mais efetuados. Por vezes, novos procedimentos são estabelecidos, mas não são de conhecimento daqueles que descrevem os processos, não sendo incluídos nas documentações disponíveis. Para determinar o funcionamento real podem ser realizadas discussões com o pessoal que executa ou é afetado pelo gerenciamento de risco ou exames de registros de desempenho operacional.

De posse dessas informações, deve-se confrontar a situação encontrada com a projetada, com a intenção precípua de determinar se os processos efetuados garantem segurança razoável do alcance dos objetivos estabelecidos.

Documentação

A extensão da documentação do processo de gerenciamento de risco varia dependendo de fatores como tamanho e complexidade das entidades. Organizações de porte geralmente possuem manuais escritos de políticas, gráficos da organização formal,

descrições de tarefas por escrito, instruções operacionais, fluxogramas de sistemas de informação, entre outros. Já organizações menores tendem a ter menos documentação escrita, mas podendo apresentar processos executados regularmente e com efetividade. Esses tipos de processos podem ser avaliados, tanto quanto os documentados, no entanto, um nível apropriado de documentação normalmente torna o monitoramento mais efetivo e eficiente.

O avaliador pode decidir documentar seu processo de avaliação. Pode partir dos documentos existentes na entidade e complementá-los com descrições de testes e análise dos processos de avaliação efetuados.

Quando a entidade pretende relatar a partes externas sobre a efetividade do gerenciamento de risco, deve considerar o desenvolvimento e guarda de documentação que suporte suas afirmações. Essa documentação pode ser útil em caso de necessidade de confirmação das afirmações feitas.

Relatando Deficiências

O termo deficiência significa uma situação no gerenciamento de risco digna de atenção. Pode representar um defeito visível, potencial ou real, ou uma oportunidade de aumentar as possibilidades de que os objetivos da entidade sejam alcançados.

Uma das melhores fontes de informação é o gerenciamento de risco em si, isto é, as atividades de monitoramento contínuo projetadas para trabalharem em tempo real. Da mesma forma, agem as avaliações separadas realizadas pelos gerentes e auditores internos.

Partes externas, tais como consumidores, vendedores, auditores externos e reguladores, também, fornecem importantes informações. Esses relatos devem ser cuidadosamente considerados, dadas suas implicações no gerenciamento de risco, e as ações apropriadas devem ser tomadas.

Com relação ao que deve ser relatado, não existe uma resposta universal. Pode-se considerar que qualquer deficiência que afete a capacidade de a entidade atingir seus objetivos estratégicos tem que ser informada àquelas pessoas em condições de executar as ações necessárias.

Para verificar o que deve ser relatado, é necessário se olhar as conseqüências do achado. Ainda, é essencial que, além de se informar as transações ou eventos particulares, se reavalie os procedimentos que potencialmente levaram à falha.

A questão de a quem relatar está relacionada aos canais de comunicação existentes na entidade. Assim é que informações geradas no curso de atividades

operacionais são, normalmente, expostas ao superior imediato. Este pode informar tanto acima ou lateralmente no seu nível na organização, mas de forma a fazer com que a informação termine com quem tem poder de ação. Canais alternativos devem existir para o informe de questões sensíveis, tais como atos impróprios ou ilegais.

Deficiências no gerenciamento de risco deveriam ser informadas não somente ao indivíduo responsável pela ação ou função envolvida, mas, pelo menos, para um nível de gerência acima. Com isso, gera-se tanto suporte, quanto vigilância relativas às ações corretivas, além do informe a outras áreas que possam vir a ser afetadas.

Questões relativas aos necessários canais de comunicação e pessoas a quem relatar deficiências devem estar explícitas em protocolos que estabeleçam, ainda, qual informação é necessária em cada nível particular da organização, de forma a prover respostas efetivas. Esses protocolos devem refletir a regra geral de que os gerentes têm que ter conhecimento de dados que afetem ações ou comportamentos de pessoas sob sua responsabilidade, assim como das informações necessárias para alcançar seus objetivos específicos. Os gerentes devem ser informados sobre as deficiências nas suas unidades com um grau de detalhe crescente à medida que se move para baixo na estrutura organizacional.

Após a exposição dos oito componentes da metodologia de Gerenciamento de Risco Empresarial, o documento do COSO discorre, ainda, sobre dois outros temas, que, pela importância, devem ser apresentados. Trata-se das "limitações do gerenciamento de risco" e dos "papéis e responsabilidades" no processo. A exposição será semelhante à anterior, de forma que os conceitos apresentados são extraídos diretamente do documento *Enterprise Risk Management Framework* do COSO.

3.9 Limitações do Gerenciamento de Risco Empresarial

Pode haver um entendimento de que o uso de metodologias de gerenciamento de risco levará a entidade a não falhar, isto é, ela sempre alcançará os seus objetivos. Essa visão, no entanto, é enganosa.

Três dimensões distintas devem ser consideradas no tocante a esse assunto. Primeiro, o risco está relacionado com eventos futuros, e o futuro é incerto. Segundo, o gerenciamento de risco opera em níveis diferentes, com respeito a objetivos diferentes. Para os objetivos estratégicos e operacionais, ele pode ajudar a assegurar que os níveis mais altos de gerência serão avisados, de modo oportuno, da extensão na qual a entidade se move para atingir esses objetivos. Mas, ele não pode fornecer nem mesmo segurança razoável de que eles serão atingidos, porque certos eventos estão, simplesmente, fora do controle gerencial. Terceiro, o gerenciamento de risco não fornece segurança absoluta em relação a nenhuma das categorias de objetivos, devido à realidade de que nenhum processo fará sempre aquilo para o qual foi projetado.

Entre esses fatores limitadores do sucesso de processos estão:

- erros de julgamento: as decisões devem ser tomadas no tempo disponível, baseadas em informações a mão e sob as pressões de conduzir um negócio;
- falhas: instruções não bem entendidas; erros devido a descuido, distração ou fadiga;
- conluio: pessoas agindo coletivamente para perpetrar ações delituosas e ocultar seus atos podem alterar dados financeiros ou outras informações gerenciais de maneira tal que não possa ser identificada pelo processo de gerenciamento de risco empresarial;
- custo x benefício: sempre existem restrições orçamentárias, de forma que qualquer entidade deve considerar os custos e benefícios de suas

decisões, incluindo aqueles relativos a respostas aos riscos e controles associados;

- objeção da gerência: significa a atitude deliberada de rejeitar as políticas e procedimentos estabelecidos por propósitos ilícitos, tais como ganho pessoal ou apresentação maquiada das condições financeiras da entidade ou da situação de conformidade. A efetividade do gerenciamento de risco é determinada pelo interesse das pessoas responsáveis pelo seu funcionamento.

3.10 Papéis e Responsabilidades

O gerenciamento de risco é executado por um grande número de partes, cada uma com importantes responsabilidades. O conselho de diretores, as gerências, a auditoria interna e outras pessoas da entidade desempenham funções e são responsáveis pelo gerenciamento de risco. Partes externas, como auditores externos e agentes regulatórios são, por vezes, associados ao gerenciamento de risco. No entanto, é fundamental distinguir que, embora prestando relevante contribuição ao processo, as partes externas não são responsáveis, em absoluto, pelo gerenciamento de risco da entidade.

Partes com Responsabilidades

Conselho de Diretores

Tem papel relevante na definição de estratégias e de objetivos de alto nível e na alocação de recursos em linhas gerais. Provê supervisão quanto ao gerenciamento de risco ao: conhecer a extensão na qual a gerência superior implantou o gerenciamento de risco na organização; conhecer e contribuir com o apetite ao risco; revisar a visão geral de risco e confronta-la com o apetite ao risco; e informar-se sobre os riscos mais relevantes e a adequabilidade das ações de resposta da gerência.

Para tanto, os membros do conselho de diretores devem ter a competência necessária, utilizar os recursos apropriados para conduzir investigações especiais e manter comunicação aberta e irrestrita com auditores internos e externos.

Gerência

O grau de responsabilidade é função do nível da gerência na estrutura organizacional.

Iniciando-se pelo diretor-presidente ou cargo equivalente, que possui a "paternidade" pelo gerenciamento de risco. É ele que dá o tom da organização (o "tom do topo"), isto é, o posicionamento que influenciará um ambiente interno positivo. É o responsável por verificar se todos os componentes do gerenciamento de risco existem. Realiza essa tarefa, geralmente, fornecendo liderança e direção aos gerentes seniores ao, em conjunto com eles, dar forma aos valores, princípios e políticas operacionais principais. Além disso, deve manter reuniões periódicas com os gerentes das principais áreas para rever suas responsabilidades, e a maneira como gerenciam suas áreas.

Gerentes seniores determinam responsabilidade pelo estabelecimento de políticas e procedimentos de gerenciamento de risco mais específicas para os funcionários responsáveis por unidades funcionais individuais.

Em qualquer processo, em um nível de responsabilização progressivo, um gerente funciona como o executivo chefe de sua esfera de responsabilidade. Também significativa é a função de chefes de funções de equipe, tais como finanças, conformidade, recursos humanos e tecnologia de informação, cujas atividades de monitoramento e controle pervagam as operações e diversas unidades da entidade.

Oficial de Risco

Algumas organizações criaram um ponto coordenador centralizado para facilitar o gerenciamento de risco. O oficial de risco, conhecido, também, como oficial-chefe de risco ou gerente de risco, trabalha com os outros gerentes no estabelecimento e manutenção de gerenciamento de risco efetivo em suas áreas. Pode ter a responsabilidade de monitorar o processo e dar assistência aos outros gerentes no informe de riscos relevantes por toda a organização, assim como servir como um canal de comunicação suplementar.

Oficiais de Finanças

Funcionários das áreas financeiras e contábeis desenvolvem importantes atividades que envolvem toda a organização. Estão envolvidos no desenvolvimento de planejamentos e orçamentos amplos e acompanham e analisam desempenhos em perspectivas operacionais, de conformidade e de divulgação.

Os responsáveis por essas áreas são pessoas chaves no estabelecimento de objetivos, na decisão de estratégias, na análise de riscos e em decisões concernentes a como mudanças que afetam a entidade serão gerenciadas. Assim, devem ter assento em qualquer reunião que envolva decisões estratégicas.

Auditores Internos

Têm um papel decisivo na avaliação da efetividade do gerenciamento de risco, inclusive com recomendação de melhoramentos. Os padrões do IIA estabelecem que o escopo de auditoria interna deve abranger gerenciamento de risco e sistemas de controle. Isso inclui a avaliação da segurança dos informes, revisão da efetividade e eficiência das operações, proteção de bens e conformidade com leis, regulamentos e contratos.

A auditoria interna não tem responsabilidade primária no estabelecimento e manutenção do gerenciamento de risco. Como visto, essa responsabilidade é dos níveis de gerência da entidade, que contam com a auditoria interna no monitoramento, no exame, na avaliação, no informe e na recomendação de melhoramentos para a adequação e efetividade do gerenciamento de risco.

Outros Funcionários

O gerenciamento de risco é, de alguma maneira, responsabilidade de todos os funcionários de uma organização, e assim deveria ser uma parte explícita e implícita de todas as descrições de funções. Virtualmente, todos os funcionários produzem informação útil e realizam ações necessárias para gerenciar riscos. Da mesma forma, todos são responsáveis por comunicar, pelos canais adequados, conhecimentos que tenham sobre problemas operacionais, não-conformidades com códigos de conduta e outra violações ou atos ilegais.

Partes Externas

Auditores Externos

Em auditorias contábeis e financeiras, o auditor externo (independente) expressa uma opinião acerca da clareza dos demonstrativos contábeis conforme princípios contábeis geralmente aceitos. Dessa forma, contribui para o alcance dos objetivos de divulgação externa da entidade.

Em muitos casos, são fornecidas informações úteis ao gerenciamento de risco ao se comunicar achados de auditoria, informações analíticas e recomendações necessárias ao alcance de objetivos, não só de divulgação, mas operacionais e de conformidade. Também podem ser comunicados achados relacionados a deficiências no gerenciamento de risco e controles internos, e recomendações para melhoria.

Legisladores e Reguladores

Afetam o gerenciamento de risco de muitas entidades, tanto mediante solicitações para estabelecimento de controles internos, quanto mediante exames de

certas entidades. Muitas das leis e regulamentos relevantes lidam, primeiramente, com riscos e controles de demonstrações financeiras. No entanto, algumas, particularmente aquelas que se destinam a organizações governamentais, lidam, também, com objetivos operacionais e de conformidade. Muitas entidades já estão, há tempos, sujeitas a solicitações legais referentes a controles internos.

Diversas agências reguladoras examinam diretamente entidades sob sua responsabilidade. Por exemplo, examinadores de bancos federais e estaduais conduzem exames em bancos e focam em aspectos relacionados ao gerenciamento de risco e controles internos. Essas agências fazem recomendações e determinações.

Partes Interagindo com a Entidade

Consumidores, vendedores e parceiros de negócios são importantes fontes de informação, que devem ter tratamento adequado, o que inclui investigar as causas das questões levantadas e corrigi-las.

Provedores de Serviços Terceirizados

Ao realizar atividades concernentes à organização, tornam-se parte dela no que se refere a riscos. Assim, devem ser estabelecidos programas de vigilância para monitorar essas atividades.

Analistas financeiros, Agências de Avaliação e Mídia

As atividades investigativas e de monitoramento desses entes podem fornecer: outras perspectivas acerca do desempenho da entidade; riscos econômicos e industriais existentes; estratégias operacionais ou financeiras inovadoras que podem melhorar o desempenho; e tendências da indústria. Essas informações podem ser obtidas mediante contatos diretos, ou, indiretamente, em análises para investidores e para o público.

4. Metodologia de Análise de Risco para Escolha de Temas de Fiscalização do TCU

O objetivo da metodologia é:

> produzir, ao final da sua aplicação em uma entidade específica ou programa de governo, um rol das principais áreas ou temas a serem objeto de ações fiscalizadoras por parte do TCU, nas suas diversas modalidades (auditorias de natureza operacional, de conformidade, de sistemas, acompanhamentos, etc.), em ordem de prioridade, explicitando as razões para tanto. ((TCU, 2003, p. 3).

Não se trata, especificamente, de uma metodologia desenvolvida para auditar o processo de gerenciamento de risco, mas para verificar as principais áreas de risco de uma instituição e propor fiscalizações nessas áreas. A comparação com a Metodologia de Gerenciamento de Risco Empresarial torna-se significativa devido à robustez dos conceitos apresentados pela metodologia do COSO.

A figura 3 apresenta o fluxograma lógico do processo utilizado na Metodologia de Análise de Risco para Escolha de Temas de Fiscalização. A seguir, será feita a explanação de cada etapa, conforme o documento do TCU, acompanhada de comentários acerca da comparação com a metodologia COSO.

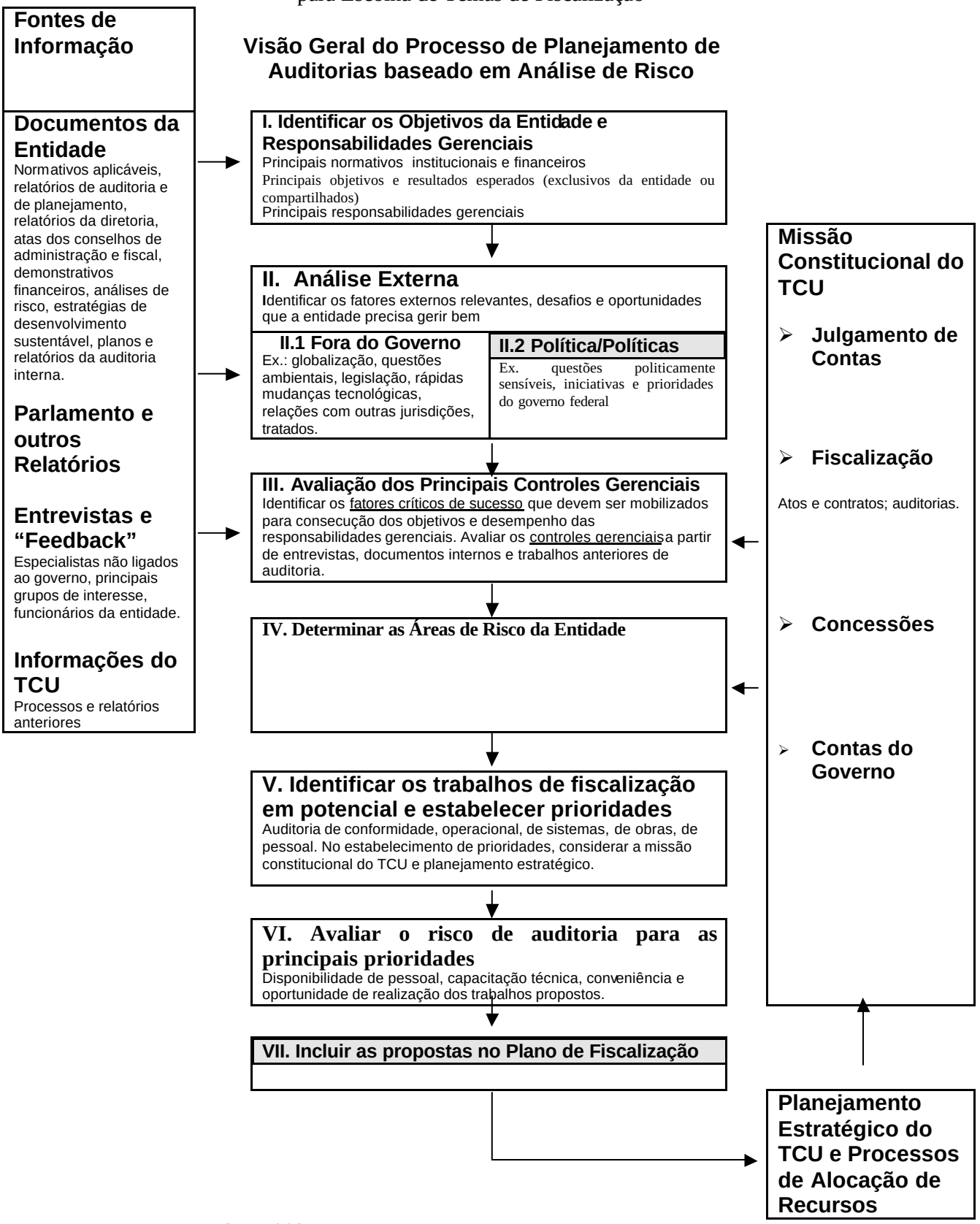
4.1 - Identificação dos Objetivos da Entidade e Responsabilidades Gerenciais - Etapa I

Pretende obter conhecimento acerca da entidade fiscalizada, focando, principalmente em sua missão, principais objetivos e principais resultados a serem alcançados.

Para tanto, deve ser feita consulta à variada documentação referente à entidade, a saber:

- normativos aplicáveis tais como lei de criação;
- documentos internos tais como: estatuto/regimento interno; organograma descrevendo as atribuições dos principais níveis gerenciais; últimas versões de planejamento estratégico, plano de ação, plano e relatório anual de atividades da auditoria interna, atas das reuniões da diretoria/conselho colegiado, e demonstrativos financeiros auditados;
- auditorias realizadas nos últimos 2 anos, inclusive recolhendo informações com equipes de fiscalização;

Fig. 3 - Fluxograma lógico do processo utilizado na Metodologia de Análise de Risco para Escolha de Temas de Fiscalização



Fonte: TCU, 2003, p.5

- página na internet;
- publicações na imprensa nos últimos 3 meses.

Também se pode obter o conhecimento necessário mediante a realização de entrevistas com os dirigentes/funcionários da organização.

Outros conhecimentos fundamentais a serem obtidos nessa fase dizem respeito à organização e funcionamento da entidade, inclusive com identificação das mais relevantes áreas e linhas de produção para a obtenção dos objetivos, assim como os principais gerentes e suas responsabilidades.

Comentários

Essa fase da metodologia corresponde às duas primeiras fases da metodologia COSO, ambiente interno e definição de objetivos.

No tocante ao ambiente interno, existem oportunidades de melhoria. Conforme o COSO, o ambiente interno de uma entidade é a base para todos os demais componentes do gerenciamento de risco. Assim, é importante aumentar a análise desse item, mormente no que se refere a questões que envolvam risco. Para tanto, deve-se verificar:

- a filosofia de gerenciamento de risco existente e o apetite ao risco;
- a existência de comunicação formal da filosofia de risco e do apetite ao risco, de forma a prover cultura de risco homogênea;
- o conselho de administração, quando existente, ou órgão similar. Sua estruturação, seu nível de independência, sua atuação e sua interação com as auditorias interna e externa;
- questões que envolvem a ética da entidade, que, embora de difícil exame, podem ser objeto de verificações objetivas, tais como: condutas passadas dos dirigentes mais importantes; políticas existentes para a concessão de benefícios para os funcionários, em especial para os de nível de gerenciamento; existência de códigos de ética ou de conduta; penalizações quando da infringência desses códigos; existência de canais para a comunicação de atos contrários aos códigos;
- as áreas chaves de autoridade e responsabilidade na estrutura organizacional, e a forma como se definem competências, autoridade e responsabilidade. Ainda, a existência de controles adequados ao grau de delegação de competência existente;

- a forma como a entidade trata o treinamento de pessoal.

Quanto à etapa de definição dos objetivos, a compatibilização com a metodologia COSO pode se processar pelo uso de terminologia semelhante. Assim, os objetivos atrelados ao alcance da missão são ditos estratégicos. A partir desses são formuladas estratégias e estabelecidos os objetivos relacionados, mais ligados à estrutura da entidade, e classificados em operacionais, de divulgação e de conformidade.

4.2 **Análise Externa – Etapa II**

Pretende identificar os fatores externos que influenciam o alcance dos objetivos, isto é, aqueles que estão fora do controle direto da entidade. Esses fatores tanto podem dificultar (riscos), quanto facilitar (oportunidades) a consecução dos objetivos.

Exemplos de fatores externos fora da ação direta do Governo são: globalização; questões ambientais; legislação; rápidas mudanças tecnológicas; relações com outras jurisdições; e tratados. Com relação direta com o Governo têm-se: questões politicamente sensíveis; e iniciativas e prioridades do Governo Federal.

Clientes, parceiros, órgãos reguladores, fornecedores, associações, sindicatos, representantes da sociedade, especialistas/acadêmicos, empresas privadas, ONGs, entre outros são considerados fontes de informação sobre fatores externos. A maneira de se obter as informações é, normalmente, a realização de entrevistas.

Comentários

Essa fase equivale à terceira fase do modelo COSO, identificação de eventos.

Há uma diferença devido ao fato de a metodologia do TCU não explicitar a identificação de eventos com fontes internas, embora a metodologia possa considerá-la implícita na fase I. Uma vantagem da metodologia COSO em considerar a identificação de eventos, de fontes internas e externas, como fase isolada no modelo é reduzir a possibilidade de negligência de eventos relevantes. Isso porque se a identificação de eventos estiver diretamente relacionada à identificação de riscos, há a tendência de se valorizar os riscos de maior probabilidade e impacto, desprezando-se os riscos dos outros três quadrantes.

Outra vantagem é potencializar a possibilidade de identificação de oportunidades, que seria bastante reduzida com a identificação imediata de riscos. Ao se identificar oportunidades, prega a metodologia COSO que elas devem ser canalizadas de volta ao processo de definição de estratégias e objetivos, com o intuito de formular ações para aproveitá-las. Assim, se no processo de análise risco para escolha de temas de fiscalização forem identificadas oportunidades, deve-se dar conhecimento à entidade, e avaliar a conveniência de se propor recomendação do Tribunal quanto a sua utilização.

Na identificação de eventos externos é interessante ter o foco não só na entidade em si, isto é, em fatores que podem afetá-la diretamente. Devem-se identificar eventos que afetem níveis de atividades, tais como vendas, produção, *marketing*, desenvolvimento tecnológico e pesquisa e desenvolvimento. Com isso, melhora o nível de avaliação de riscos em grandes áreas de negócio, que podem vir a afetar a entidade.

Identificados os eventos, deve-se verificar possíveis inter-relações, que podem afetar os riscos.

Outra possibilidade é a categorização de eventos, em, por exemplo, derivados de fatores internos e externos. Com isso, melhora o entendimento de inter-relacionamentos, pode-se verificar, de forma mais abrangente, a qualidade do trabalho até então realizado, e se ganha uma visão mais integrada dos riscos/oportunidades.

4.3 **Avaliação dos Controles Gerenciais - Etapa III**

Visa a identificação das áreas ou dos processos internos mais relevantes para o alcance dos objetivos da entidade, chamados de fatores críticos de sucesso, e a avaliação da qualidade dos controles gerenciais em relação a esses setores.

Não é feita auditoria nos controles, mas a verificação de existência e exame de potenciais possibilidades de falhas. Os principais controles de uma entidade estão relacionados a processos e estruturas de supervisão, que permitam aos gerentes acompanhar o desempenho da instituição, e a eficiência e a eficácia com que está atingindo os objetivos determinados.

A existência de controles eficientes é fator essencial para gerenciamento dos riscos, com a conseqüente redução do nível de exposição ao risco da entidade. Ao se avaliar os principais controles gerenciais avalia-se, na verdade, a capacidade dos dirigentes da empresa em monitorar e gerenciar os riscos.

A avaliação dos controles é feita com entrevistas, e com análises de documentos internos e de relatórios de auditorias anteriores.

Determinação das áreas Estratégicas de Risco da Entidade - Etapa IV

Com base nas informações levantadas nas etapas anteriores, identifica as principais áreas de risco. Os principais aspectos que podem apontar para uma área de risco são:

- relevância da área em relação aos objetivos da entidade;
- inexistência de processos ou sistemas que permitam a gerência acompanhar o andamento de atividades relevantes para os objetivos (controles gerenciais);
- potenciais falhas ou fragilidades nos controles existentes;
- existência de fatores externos de risco;
- dificuldade de responder tempestivamente aos fatores externos;
- incidência de falhas apontadas em trabalhos anteriores.

Comentários

Há aqui uma grande diferença conceitual entre os modelos.

A seqüência de etapas estabelecida pelo modelo COSO, após definidos os principais objetivos, e verificados os eventos com efeito potencialmente negativo, é:

- estabelecer a probabilidade de ocorrência e o provável impacto em caso de ocorrência do evento negativo (avaliação de riscos);
- definir ações (respostas aos riscos) para os riscos de binômio probabilidade x impacto mais relevantes, de forma a minimizar esse binômio e ajustar o risco residual a um nível aceitável, chamado de tolerância ao risco;
- estabelecer controles, intimamente ligados às ações de resposta ao risco, de forma a acompanhar a eficácia e a oportunidade de execução dessas ações.

Inicialmente, a metodologia COSO não foca, exatamente em áreas de risco, mas sim em eventos de risco. Assim, mesmo que uma atividade ou área seja de grande relevância para o alcance dos objetivos estratégicos de uma instituição, só se falará em risco nessa área, se houver eventos, de fontes internas ou externas, com binômio probabilidade de ocorrência x impacto significativo.

Definidos os eventos de maior risco, é indispensável a fase de avaliação de respostas aos riscos, pois, na verdade, elas constituem a própria ação da instituição no sentido de reduzir o nível de exposição ao risco. As atividades de controle devem ser encaradas como conseqüências das respostas aos riscos, construídas diretamente dentro do processo de gerenciamento. Isso minimiza a noção de que atividades de controle devam existir meramente por obrigação, e cria controles realmente eficazes.

Não são as atividades de controle que reduzem o nível de exposição ao risco da entidade, e sim as respostas aos riscos estabelecidas. Os controles existem para garantir que as respostas escolhidas estão sendo executadas a contento, e é isso que reduz a exposição ao risco.

Portanto para entender o porquê de algum tipo de controle, há que se conhecer a ação controlada, a resposta ao risco. Por esse motivo, não se deve inverter as fases, avaliando-se primeiro os controles, e depois se definindo os riscos principais.

Como o estabelecimento de respostas aos riscos é tarefa eminentemente gerencial, não cabe ao TCU interferir no processo de escolha por parte dos gerentes. Mas, cabe ao Tribunal verificar a existência de respostas aos principais riscos, e analisar as respostas aos riscos escolhidas, se elas são pertinentes e suficientes para levar o risco residual à tolerância estabelecida. Em caso negativo, cabe ao Tribunal determinar que a entidade tome as providências que julgar necessárias para minimizar o risco à

consecução de seus objetivos estratégicos. Lembrar que esses objetivos estão atrelados à missão da entidade, que, via de regra, é um mandato legal.

O mesmo pensamento vale para as atividades de controle definidas pela instituição. Deve-se verificar se elas estão relacionadas às principais ações de resposta aos riscos, se são adequadas ao que se destinam, e se estão sendo realizadas conforme projetadas. Se não, cabe ao Tribunal determinar que a entidade tome as providências que julgar necessárias para estabelecer, efetivamente, atividades de controle às ações de resposta aos principais riscos que possam impedir o alcance de sua missão legal.

4.4 Priorização das Áreas de Risco e Apontamento do Tipo de Fiscalização Requerida - Etapa V

Objetiva definir temas de fiscalização a partir da identificação das principais áreas de risco. Para cada área identificada, deverá ser proposta uma ação de fiscalização adequada, explicitando-se as razões motivadoras dos temas escolhidos e a priorização proposta para a execução das fiscalizações.

Deve-se considerar a possibilidade de uma determinada área de risco não vir a ser objeto de fiscalização por já estar sendo satisfatoriamente controlada pela instituição, ou por já estar sendo objeto de controle pelo Tribunal ou outro órgão afim.

Também, deve-se verificar se a fiscalização a ser proposta se adéqua à missão institucional, ao planejamento estratégico e às metas do Tribunal.

Por fim, é necessário discutir com os titulares das unidades técnicas responsáveis pela realização das fiscalizações a conveniência e a oportunidade de realização dos trabalhos.

Avaliação do Risco das Fiscalizações Sugeridas - Etapa VI

Objetiva avaliar os riscos envolvidos na realização das fiscalizações propostas. Observa-se a existência de pessoal capacitado, a relevância de cada tema, e a conveniência de realização. Essas análises devem ser feitas em conjunto com as unidades técnicas responsáveis pelas fiscalizações propostas.

Submissão das Propostas ao Plenário - Etapa VII

Refere-se à inclusão das propostas de fiscalização no plano de fiscalização do Tribunal para posterior submissão à aprovação do Plenário, nos termos do art. 244 do Regimento Interno do TCU.

Comentários

Um dos motivos expostos para a não realização de proposta de fiscalização é a existência de controle adequado, seja pela própria entidade, seja por algum ente de controle, incluindo o TCU. No entanto, não há como se saber se o controle efetuado é efetivo a não ser pela realização de um processo de auditoria nesse controle.

Duas etapas da metodologia COSO não são contempladas na metodologia do TCU, ao menos, explicitamente. Trata-se de “informação e comunicação” e “monitoramento”.

O item “informação e comunicação” possui relação imediata com o ambiente interno da instituição. Portanto é possível que ao realizar a primeira fase da metodologia TCU, na qual se identifica características intrínsecas da entidade, alguns dos aspectos de informação e comunicação sejam vistos. De qualquer maneira, explicita-se algumas das verificações necessárias:

- a existência de um sistema estruturado de informação de dados;
- os critérios para projeto da arquitetura de sistemas de informação e aquisição de tecnologia;
- se a entidade realiza, e como realiza, a consulta e utilização de dados históricos e atuais para gerenciamento de risco;
- se é dado tratamento de análise de risco aos sistemas de informação;
- a existência e a qualidade de programa de gerenciamento total de dados;
- se a estrutura de comunicação interna existente é capaz de: garantir o conhecimento da importância e relevância de um gerenciamento de risco efetivo; informar a filosofia de risco, o apetite ao risco e a tolerância ao risco da entidade; implementar e manter uma linguagem comum de risco; e notificar aos funcionários sobre seu papel e responsabilidades no gerenciamento de risco;
- a existência de canais de comunicação internos e as políticas para sua utilização;
- a forma como se dá a comunicação entre o conselho de diretores e a alta gerência.

Ainda, no caso da existência de sistemas de ERP, deve-se verificar a metodologia de implementação, o grau de satisfação dos usuários, possíveis falhas de segurança e integridade dos dados. A situação desejada nesses casos é a realização prévia de auditoria de TI no sistema de ERP, dada a sua importância e abrangência para a entidade.

O item “monitoramento” é de importância especial. A existência de um sistema de monitoramento eficaz por parte da entidade é fator relevante na redução do risco de

controle, dada a capacidade incrementada de retroalimentação e possível melhoria das atividades de controle.

Assim, deve-se verificar a forma como a entidade monitora seu gerenciamento de risco, se existem atividades corriqueiras de monitoramento (monitoramento contínuo) ou se o monitoramento é efetuado somente em separado. Se houver auditoria interna na entidade, ou via sistema de controle interno do Poder Executivo Federal, deve-se averiguar se é realizado algum tipo de trabalho relativo à monitoração do gerenciamento de risco.

Entidades com monitoramento contínuo de gerenciamento de risco possuem, ainda, uma grande fonte de pesquisa para se conhecer mais detalhadamente suas características.

Alguns fatores são motivos para realização de monitoramentos em separado, e devem ser cotejados pelo controle externo quando da planificação de novas fiscalizações. Entre eles estão: mudanças nas estratégias principais ou na gerência superior; grandes aquisições ou vendas; alterações significativas nas condições econômicas ou políticas; e mudanças significativas nas operações ou nos métodos de processamento de informações.

É interessante se estudar a possibilidade de realizar as avaliações em separado do controle externo mediante o uso de auto-avaliações (*csa – control self assessment*). Seriam distribuídos regularmente e oficialmente relatórios que os gerentes de cada área deveriam responder ao TCU com questões focadas no gerenciamento de risco. Por amostragem, ou por critérios de risco, realizar-se-iam auditorias para conferência.

5. Conclusão

Conforme frisado no item Materialidade, Risco de Auditoria e Evidência da Revisão de Literatura, a Metodologia de Gerenciamento de Risco Empresarial do COSO é, do ponto de vista da auditoria, um modelo que objetiva entender, avaliar e gerenciar os riscos inerentes de uma entidade.

Da mesma forma, a Metodologia de Análise de Risco para Escolha de Temas de Fiscalização empregada pela TCU pretende analisar os riscos inerentes de uma instituição, e a forma com que são geridos, para propor áreas e temas para a ação fiscalizatória do Tribunal.

A idéia ao comparar essas duas metodologias foi de se utilizar os conceitos mais atuais da metodologia COSO para agregar valor ao esforço realizado pelo Tribunal.

Uma interessante constatação deste trabalho está relacionada à evolução do conceito de controles internos apresentada pelo documento do COSO. Um dos pensamentos dessa instituição ao lançar a metodologia foi a de agregar conceitos em uma terminologia comum sobre gerenciamento de risco.

De certa forma, a teoria apresentada pelo COSO modifica o entendimento de controles internos exposto na Revisão de Literatura, inclusive o entendimento do próprio COSO expresso no documento *Internal Control – Integrated Framework*, de 1992. Ao incluir o conceito de ação de resposta ao risco e relacionar as atividades de controle diretamente a essas ações, criou-se uma nova dimensão, certamente mais apropriada à realidade de gerenciamento de uma instituição. Como discutido, não são as atividades de controle que reduzem o risco, mas as ações de resposta ao risco. E os controles servem para garantir a efetividade e oportunidade dessas ações.

Ao se comparar as metodologias do TCU e do COSO, não houve a intenção de se definir uma nova metodologia. Principalmente no tocante a procedimentos de execução, tais quais os existentes no documento do TCU consultado, que define a implementação da metodologia para um instrumento de fiscalização levantamento, com planejamento, execução e relatório.

Evidentemente, se as considerações formuladas nesta monografia forem consideradas úteis, há que se expandir o trabalho de forma a definir novos procedimentos de execução. Esses podem, inclusive, serem relacionados a outros

instrumentos de fiscalização, tais como auditorias de natureza operacional de avaliação de gestão ou de desempenho de instituições e acompanhamentos.

De uma maneira geral, pode-se dizer que a Metodologia de Análise de Risco para Escolha de Temas de Fiscalização empregada pelo TCU apresenta diferenças em relação aos conceitos da Metodologia de Gerenciamento de Risco Empresarial definidos pelo COSO. A maior está na avaliação dos principais controles gerenciais sem realizar uma avaliação prévia dos riscos e das respostas aos riscos correspondentes.

Conforme explicado, essa diferença carrega em si um descasamento de conceitos, quando a metodologia do TCU (2003, p.6) explicita que "a existência de controles eficientes é fator essencial para gerenciamento dos riscos, com a conseqüente redução do nível de exposição ao risco da entidade". Pelos conceitos defendidos pelo COSO, são as ações de resposta aos riscos que reduzem o nível de exposição ao risco da instituição, servindo os controles como garantia de execução a contento dessas ações de resposta aos riscos.

Outra constatação é a inexistência nos documentos do TCU consultados de definições formais a respeito de risco de auditoria e seus componentes. Na verdade, o que se observa é a ausência da consideração, principalmente, do conceito de risco de detecção. Não há no processo de fiscalização exercido pelo Tribunal a explicitação de que a atividade de auditoria, como qualquer outra, está sujeita a riscos, e que, portanto, a opinião dada não apresenta infalibilidade.

É necessária a realização de estudos que venham a incorporar no processo de auditoria do Tribunal o conceito de nível de confiança, refletindo a garantia dada pelo auditor do grau de certeza de suas afirmações. Evidente, que a função judicante do TCU deve ser considerada, constituindo, um entrave a ser analisado.

No entanto, há que se obter meios de se informar ao interessado nos julgamentos realizados a real expressão da opinião emitida mediante o processo de auditoria, que, sem sombra de dúvida, nunca apresenta certeza absoluta. Deve se destacar, contudo, que essa certeza absoluta também não é possível nos processos judiciais, nos quais se trabalha com a busca da reconstituição da verdade, e não com a verdade real e absoluta, esta última nem sempre possível de ser atingida.

REFERÊNCIAS

ARAÚJO, I.P.S. *Introdução à Auditoria*: breves apontamentos de aula – aplicáveis à área governamental e aos programas de concursos públicos. Salvador: Egba, 1998.

ATTIE, W. *Auditoria Interna.* São Paulo: Atlas, 1992.

_____. *Auditoria*: conceitos e aplicações. 3. ed. São Paulo: Atlas, 1998.

BOYNTON, W. C.; JONNSON, R. N.; KELL, W. G. *Auditoria*. São Paulo: Atlas, 2002.

COCURULLO, A. *Gestão de riscos corporativos*; Riscos Alinhados com Algumas Ferramentas de Gestão: Um Estudo de Caso. São Paulo: Scortecci, 2002.

_____. *Risco e Auditoria*: material de curso ministrado na Pós–Graduação em Controle Externo do Instituto Serzedello Corrêa. Brasília, 2003.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION – COSO. *Internal Control – Integrated Framework*: Executive Sumary. Washington, 1992.

_____. *Enterprise Risk Management Framework*: executive summary: draft. Washington, 2003a.

_____. *Enterprise Risk Management Framework*: framework: draft. Washington, 2003b.

CONSELHO FEDERAL DE CONTABILIDADE - CFC. *NBC T 11 – Normas de Auditoria Independente das Demonstrações Contábeis.* Brasília. 1997.

FLORENTINO, A.M. *Auditoria Contábil*. Rio de Janeiro: Fundação Getúlio Vargas, 1975.

GOMES, A.L.O. *Auditoria Contábil-Financeira*: material de curso ministrado na Pós–Graduação em Controle Externo do Instituto Serzedello Corrêa. Brasília, 2003.

HOUAISS, A. *Dicionário Eletrônico Houaiss da Língua Portuguesa.* Versão 1.0. 2001

INTERNATIONAL FEDERATION OF ACCOUNTANTS - IFAC. *Codification of International Standards on Auditing and International Auditing Practice Statements.* Nova York. 2001.

INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS – INTOSAI. *Guidelines for Internal Control Standards.* Viena. 1992.

_____. *Internal Control* :Providing a Foundation for Accountability in Government. Viena. 2001

ROZO, J.D. *Controle Interno como Variável Explicativa do Sucesso Empresarial.* São Paulo. Acesso em 10 out. 2003.

SÁ. A.L. *Curso de Auditoria.* 10. ed. São Paulo: Atlas. 2002.

TRIBUNAL DE CONTAS EUROPEU. *Políticas e Normas de Auditoria do Tribunal*.2.ed.Luxemburgo, 2002.

TRIBUNAL DE CONTAS DA UNIÃO - TCU. *Glossário de Termos Comuns Utilizados no Âmbito do Controle Externo-Acordo Brasil/Portugal*. Brasília, 1995.

_____. *Roteiro de Aplicação da Metodologia de Análise de Risco para Escolha de Temas de Fiscalização*. Brasília, 2003.

TRIBUNAL DE CONTAS DE PORTUGAL. *Manual de auditoria e de Procedimentos*: volume I. Lisboa, 1999.